Summit WM-Series WLAN Switch and Altitude Access Point Software Version 1.0 User Guide

Extreme Networks, Inc.
3585 Monroe Street
Santa Clara, California 95051
(888) 257-3000
http://www.extremenetworks.com

Published: September 2005
Part number: 100198-00 Rev 03

Alpine, Altitude, BlackDiamond, EPICenter, Ethernet Everywhere, Extreme Ethernet Everywhere, Extreme Networks, Extreme Turbodrive, Extreme Velocity, ExtremeWare, ExtremeWorks, GlobalPx Content Director, the Go Purple Extreme Solution Partners Logo, ServiceWatch, Summit, the Summit7i Logo, and the Color Purple, among others, are trademarks or registered trademarks of Extreme Networks, Inc. or its subsidiaries in the United States and other countries. Other names and marks may be the property of their respective owners.

© 2005 Extreme Networks, Inc. All Rights Reserved.

Specifications are subject to change without notice.

The ExtremeWare XOS operating system is based, in part, on the Linux operating system. The machine-readable copy of the corresponding source code is available for the cost of distribution. Please direct requests to Extreme Networks for more information at the following address:

Software Licensing Department
3585 Monroe Street
Santa Clara CA 95051

NetWare and Novell are registered trademarks of Novell, Inc. Merit is a registered trademark of Merit Network, Inc. Solaris and Java are trademarks of Sun Microsystems, Inc. F5, BIG/ip, and 3DNS are registered trademarks of F5 Networks, Inc. see/IT is a trademark of F5 Networks, Inc.

sFlow® is a registered trademark of InMon Corporation.

All other registered trademarks, trademarks and service marks are property of their respective owners.

Table of Contents

About this Guide 9

Who should use this guide 9
What is in this guide 9
Formatting conventions 10
Documentation feedback 10
Protocols and standards 11
Regulatory information 11

Chapter 1: The Summit WM-Series Switch Software solution 13

What is the Summit WM-Series Switch Software system? 13
Conventional wireless LANS 13
The Summit WM-Series Switch Software solution 14
Summit WM-Series Switch Software and your network 17
Components of the solution: a summary 17
Network traffic flow 18
Network security 19
Authentication 19
Privacy 19
Interaction with wired networks: Wireless Mobility Access Domain 20
Static routing and routing protocols 20
Policy: packet filtering 21
Mobility and roaming 21
Availability 22
Quality of Service (QoS) 22

Chapter 2: Summit WM-Series Switch: Startup 23

Summit WM-Series Switch features and installation 23
Installing the Summit WM-Series Switch 24
First-time setup of Summit WM-Series Switch 24
Management port first-time setup 24
Changing the Management Port IP address: web browser method 25
Adding the Summit WM-Series Switch to your enterprise network 27
The graphical user interface (GUI): overview 28

Chapter 3: Summit WM-Series Switch Software configuration 31

Configuration steps: overview 31
Enabling the product key 31
Setting up the data ports 32
Setting up static routes 35
Setting up OSPF Routing 36
Filtering at the interface level 38
Port-based exception filters: built-in 39
Port-based exception filters: user defined 39

Chapter 4: Altitude AP: startup 41

Altitude AP features 41
Installing the Altitude APs 43
Connecting and powering the Altitude AP 44
Discovery and registration: Altitude AP registration settings 44
Discovery and registration 46
Discovery steps 46
Altitude AP access approval 49
Configuring properties and radios 51
View and modify properties of registered Altitude APs 51
View and modify the radio settings of registered Altitude APs 52
Adding a Altitude AP manually 56
Altitude AP static configuration: branch office deployment 57
Auto Cell software 58

Chapter 5: WM Access Domain Services (WM-AD): Introduction 61

Overview 61
What is a WM-AD? 62
Topology of a WM-AD 62
Network assignment and authentication for a WM-AD 63
Authentication with SSID network assignment 63
Authentication with AAA (802.1x) network assignment 64
Filtering for a WM-AD 64
Privacy on a WM-AD: WEP and WPA 66
Setting up a new WM-AD 66
Global Settings for a WM-AD 68

Chapter 6: WM Access Domain Configuration 71

Topology for a WM-AD 71
Topology for a WM-AD for Captive Portal 71
Topology for a WM-AD for AAA 75
Authentication for a WM-AD 76
Authentication for a WM-AD for Captive Portal 77
Authentication for a WM-AD for AAA 82
MAC-based authentication for a WM-AD 82
Accounting for a WM-AD 84
RADIUS Policy for a WM-AD 84
RADIUS Policy for Captive Portal 85
RADIUS Policy for AAA and AAA groups 85
Filtering rules for a WM-AD 86
Filtering rules for an exception filter 87
The non-authenticated filter for Captive Portal 87
Filtering rules for a Filter ID group 90
Filtering rules for a default filter 92
Filtering Rules for an AAA Group WM-AD 94
Filtering rules between two wireless devices 94
Multicast for a WM-AD 95

Privacy for a WM-AD....96
Privacy for a WM-AD for Captive Portal....96
Privacy for a WM-AD for AAA....97
A WM-AD with no authentication....100
A WM-AD for voice traffic....101

Chapter 7: Summit WM-Series Switch Configuration: Availability and Mobility....103

Availability....103
Mobility and the WM-AD Manager....107
VW-AD Manager and VW-AD Agent: Background....107

Chapter 8: Summit WM-Series Switch: configuring other functions....111

Management users....111
Network time....112
Check Point event logging....113
Setting up SNMP....115
MIB support....115
Enabling SNMP on the Summit WM-Series Switch....116

Chapter 9: Setting up third-party access points....119

Chapter 10: Summit Spy: detecting rogue access points....123

Overview....123
Enabling the Analysis and RFDC Engines....124
Summit Spy: running scans....125
The Analysis Engine....126
Viewing the Scanner Status report....130

Chapter 11: Ongoing operation....131

Altitude AP maintenance: software....131
Altitude AP client management....133
Client disassociate....134
Client blacklist....135
Summit WM-Series Switch software maintenance....137
Summit WM-Series Switch Software logs and traces....140
Viewing log, alarm and trace messages....141
Reports and displays....144
View displays....144
View reports....146

Glossary....147

Appendix A: Summit WM-Series Switch Software system states and LEDs....167

Summit WM-Series Switch system states and LEDs....167
Altitude AP system states....168

Appendix B: CLI command reference....169

Appendix C: DHCP, SLP, and Option 78 reference 173
Service Location Protocol (SLP) (RFC2608) 174
DHCP Options for Service Location Protocol (RFC2610) 174
SLP Directory Agent Option (Option 78) 174
SLP Service Scope Option (Option 79) 175

Appendix D: Reference lists of standards 177
RFC list 177
802.11 standards list 178

Appendix E: Support for Altitude AP 181
Altitude AP diagnostics by Telnet 181

Appendix F: RADIUS Attributes 183
RADIUS Vendor-Specific Attributes (VSAs) 183
RADIUS Accounting 184
Account-Start Packet 184
Account-Stop/Interim Packet 185
Termination Codes 186

Appendix G: Logs and Events 187
Overview 187
Critical 187
ACCESSPOINT 187
CDR_COLLECTOR 191
CONFIG_MANAGER 191
EVENT_SERVER 192
LANGLEY 194
RADIUS_ACCOUNTING 194
RADIUS_CLIENT 194
RF_DATA_COLLECTOR 195
RU_MANAGER 195
SECURITY_MANAGER 196
STARTUP_MANAGER 197
STATS_SERVER 198
VNMGR 199
Major 200
ACCESSPOINT 200
CDR_COLLECTOR 201
CLI 202
CONFIG_MANAGER 203
CPDP_AGENT_ID 203
EVENT_SERVER 204
LANGLEY 205
NSM_SERVER 205
OSPF_SERVER 206
PORT_INFO_J_MANAGER 206
RADIUS_ACCOUNTING 206
RADIUS_CLIENT 206
REDIR_ID 207
RF_DATA_COLLECTOR 207

RU_MANAGER 208
SECURITY_MANAGER 208
VNMGR 210

Appendix H: Regulatory Information 213

Summit WM100 (15945), Summit WM1000 (15937) 213
Safety 213
Emissions 214
Environmental Operating Conditions for Summit WM100/1000 and Altitude 350-2 214
Altitude 350-2 Integrated Antenna AP (15938), Altitude 350-2 Detachable Antenna AP (15939) .215
United States - FCC Declaration of Conformity Statement 215
Conditions Under Which a Second party may replace a Part 15 Unlicensed Antenna 217
FCC RF Radiation Exposure Statement 217
Department of Communications Canada Compliance Statement 217
European Community 218
Declaration of Conformity with regard to R&TTE Directive of the European Union 1999/5/EC ... 218
Conditions of Use in the European Community 219
Permitted 5 GHz Channels for the European Community 221
European Spectrum Usage Rules 221
Declarations of Conformity 223
Certifications of Other Countries 224

Index 225

About this Guide

This guide describes how to install, configure, and manage the Summit WM-Series Switch Software.

Who should use this guide

This guide is a reference for system administrators who install and manage the Summit WM-Series Switch Software.

What is in this guide

This guide contains the following chapters:

- About this Guide describes the target audience and content of the guide, the formatting conventions used in it, and how to provide feedback on the guide.
- Chapter 1 provides an overview of the product, its features and functionality.
- Chapter 2 describes how to perform the installation and first-time setup of the Summit WM-Series Switch.
- Chapter 3 describes setting up the initial configuration, as well as configuring the data ports and defining routing.
- Chapter 4 tells how to install the Altitude AP, how it discovers and registers with the Summit WM-Series Switch, how to view and modify the radio configuration, and how to enable Dynamic Radio Frequency Management.
- Chapter 5 provides an overview of WM Access Domain Services (WM-AD), the mechanism by which the Summit WM-Series Switch Software controls and manages network access.
- Chapter 6 gives detailed instructions in how to configure a WM-AD, its topology, authentication, accounting, RADIUS policy, multicast, filtering and privacy. Both Captive Portal and AAA types of WM-AD are described.
- Chapter 7 describes how to set up the features that provide availability in the event of a Summit WM-Series Switch failover, and mobility for a wireless device user.
- Chapter 8 includes functions, such as user privileges, network time, Check Point event logging and SNMP.
- Chapter 9 describes how to use the Summit WM-Series Switch Software features with third-party Altitude APs.
- Chapter 10 explains the security tool that scans for, detects and reports on rogue access points.
- Chapter 11 describes maintenance activities, such as software upgrades on both the Summit WM-Series Switch and the Altitude AP. This chapter also includes information on the logs, traces, reports and displays available.
- Appendix A provides a reference on the LED displays and their significance.
- Appendix B provides a list of the CLI command line syntax.

- Appendix C provides background information on how the discovery process uses these network services.
- Appendix D provides a reference list of RFCs supported.
- Appendix E provides information on a support tool.
- Appendix F provides a reference list of the RADIUS Attributes that are supported by the Summit WM-Series Switch Software.
- Appendix G provides a reference list of the log and event messages.
- Appendix H provides regulatory information for the Summit WM-Series Switch and the Altitude 350-2 Wireless Access Point.

This guide also contains a glossary of standard industry terms used in this guide.

Formatting conventions

The Summit WM-Series Switch Software documentation uses the following formatting conventions to make it easier to find information and follow procedures:

- **Bold** text is used to identify components of the management interface, such as menu items and section of pages, as well as the names of buttons and text boxes.

  For example: Click **Logout**.
- `Monospace` font is used in code examples and to indicate text that you type.

  For example: `Type https://<hls-address>[:mgmt-port>]`
- The following symbols are used to draw your attention to additional information:

NOTE

Notes identify useful information that is not essential, such as reminders, tips, or other ways to perform a task.

WARNING!

Warnings identify essential information. Ignoring a warning can lead to problems with the application.

Documentation feedback

If you have any problems using this document, please contact your next level of support:

- Customers should contact the Extreme Networks Technical Assistance Center (TAC).

When you call, please have the following information ready. This will help us to identify the document that you are referring to.

- Title: Summit WM-Series WLAN Switch and Altitude Access Point Software Version 1.0 User Guide
- Part Number: 100198-00 Rev 01

Protocols and standards

Appendix D lists the protocols and standards supported by the Summit WM-Series Switch Software. These lists include the Requests for Comment (RFCs) of the Internet Engineering Task Force (IETF) and the 802.11 standards developed by the Institute of Electrical and Electronics Engineers (IEEE).

Regulatory information

Appendix H provides regulatory information for the Summit WM-Series Switch and the Altitude 350-2 Wireless Access Point.

1 The Summit WM-Series Switch Software solution

The next generation of Extreme Networks wireless networking devices provides a truly scalable WLAN solution. Extreme Networks Altitude APs are thin access points that are controlled through a sophisticated network device, the Summit WM-Series Switch. This solution provides the security and manageability required by enterprises and service providers alike.

The Summit WM-Series Switch Software system is a highly scalable wireless local area network (WLAN) solution developed by Extreme Networks. Based on a third generation WLAN topology, the Summit WM-Series Switch Software system makes wireless practical for medium and large-scale enterprises and for service providers.

The Summit WM-Series Switch Software system provides a secure, highly scalable, cost-effective solution based on the IEEE 802.11standard. The solution is intended for enterprise networks operating on many floors in more than one building, as well as in public environments such as airports and convention centers that require more than two access points.

This section provides an overview of the fundamental principles of the Summit WM-Series Switch Software system: what it is, how it works, and its advantages.

What is the Summit WM-Series Switch Software system?

The Summit WM-Series Switch Software system replaces the conventional access points used in wireless networking with two network devices that work as a system:

- Summit WM-Series Switch: A network device that provides smart centralized control over the elements (Altitude APs) in the wireless network.
- Altitude APs: The access points for 802.11 clients (wireless devices) in the network, controlled by the Summit WM-Series Switch. The Altitude AP is a "fit access point" because its wireless control is handled by the Summit WM-Series Switch. The Altitude AP is a dual-band access point, with both 802.11a and 802.11b/g radios.

Together, the Summit WM-Series Switch Software products enable a radically simplified new approach to setting up, administering and maintaining a WLAN. Summit WM-Series Switch Software provides a Layer 3 IP routed WLAN architecture. This architecture can be implemented over several subnets without requiring the configuration of virtual local area networks (VLANs).

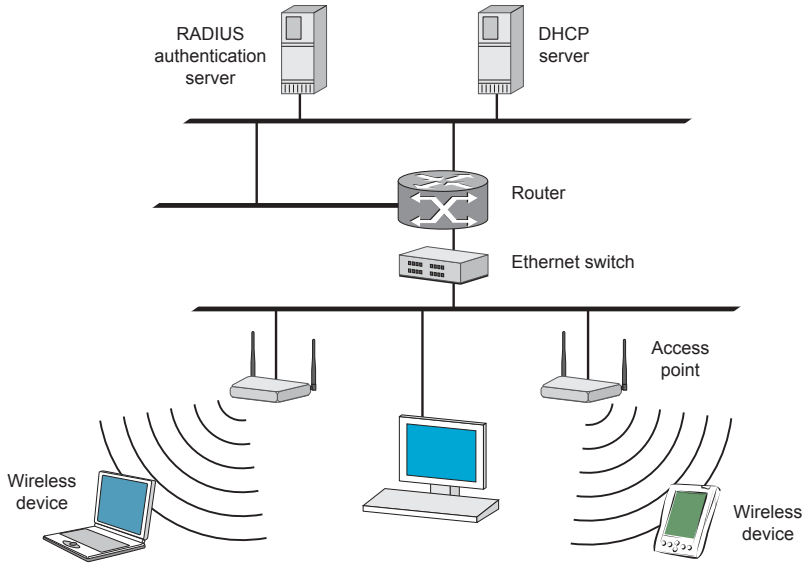
Conventional wireless LANS

At its simplest, wireless communication between two or more computers requires that each one is equipped with a receiver/transmitter – a WLAN Network Interface Card (NIC) – capable of exchanging digital information over a common radio frequency. This is called an *ad hoc* configuration. An *ad hoc* network allows wireless devices to communicate together. This is an independent basic service set (IBSS).

An alternative to the ad hoc configuration is the use of an *access point*. This may be a dedicated hardware router or a computer running special software. Computers and other wireless devices communicate with each other through this access point. The 802.11 standard defines Access Point communications as devices that allow wireless devices to communicate with a "distribution system". This is a basic service set (BSS) or infrastructure network.

For the wireless devices to communicate with computers on a wired network, the access points must be connected into the wired network, and provide access to the networked computers. This is called *bridging*. Clearly, there are security issues and management scalability issues in this arrangement.

Figure 1: Standard wireless network solution



The wireless devices and the wired networks communicate with each other using standard networking protocols and addressing schemes. Most commonly, Internet Protocol (IP) addressing is used.

While this topology works well enough for small installations, as the network grows the difficulty of setting up and administering all the individual access points expands as well. When the expanding network has to cope with a large number of wireless users all signing on and off at random times, the complexity grows rapidly. Imagine, for example, a university library filled with professors and students – all equipped with laptops. Or a conference full of delegates and exhibitors.

Clearly, there must be a better way than setting up each access point individually.

The Summit WM-Series Switch Software solution

The Summit WM-Series Switch Software solution consists of two devices:

- The Summit WM-Series Switch is a rack-mountable network device designed to be integrated into an existing wired Local Area Network (LAN). It provides centralized control over all access points (both Altitude APs and third-party access points) and manages the network assignment of wireless device clients associating through access points.
- The Altitude AP is a wireless LAN *fit access point* (IEEE 802.11) provided with unique software that allows it to communicate only with a Summit WM-Series Switch. (A *fit access point* handles the radio

frequency (RF) communication but relies on a controller to handle WLAN elements such as authentication.) The Altitude AP also provides local processing such as encryption.

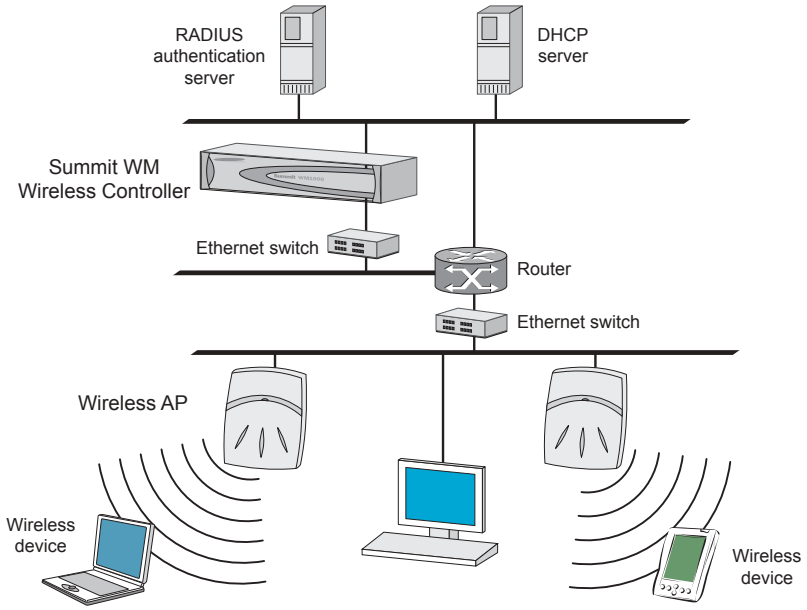
This architecture allows a single Summit WM-Series Switch to control many Altitude APs, making the administration and management of large networks much easier.

There can be several Summit WM-Series Switchs in the network, each with its set of registered Altitude APs. The Summit WM-Series Switchs can also act as backups to each other, providing stable network availability.

In addition to the Summit WM-Series Switchs and Altitude APs, the solution requires three other components, which are standard for enterprise and service provider networks:

- **RADIUS Server** (Remote Access Dial-In User Service) (RFC2865 and RFC2866), or other authentication server. Assigns and manages ID and Password protection throughout the network. Used for authentication of the wireless users.
- **DHCP Server** (Dynamic Host Configuration Protocol) (RFC2131). Assigns IP addresses, gateways and subnet masks dynamically. Also used by the Altitude APs to discover the location of the Summit WM-Series Switch during the initial registration process.
- **SLP** (Service Location Protocol) (RFC2608) supported on the DHCP server, when SLP is used as part of the discovery mechanism.

Figure 2: Summit WM-Series Switch Software solution



The Summit WM-Series Switch appears to the existing network as if it were an access point, but in fact one Summit WM-Series Switch controls many Altitude APs.

The Summit WM-Series Switch has built-in capabilities to recognize and manage the Altitude APs. The Summit WM-Series Switch activates the Altitude APs, enables them to receive wireless traffic from wireless devices, processes the data traffic from the Altitude APs and forwards or routes that data traffic out to the network. This processing includes authenticating requests and applying access policies.

Simplifying the Altitude APs makes them:

- cost-effective
- easy to manage
- easy to deploy

Putting control on an intelligent centralized Summit WM-Series Switch enables:

- centralized configuration, management, reporting, maintenance
- high security
- flexibility to suit enterprise
- scalable and resilient deployments with a few Summit WM-Series Switches controlling hundreds of Altitude APs

Here are some of the Summit WM-Series Switch Software system advantages:

Table 1: Advantages of the Summit WM-Series Switch Software system

Scales up to Enterprise capacity	One Summit WM-Series Switch controls as many as 200 Altitude APs. In turn each Altitude AP can handle up to 127 wireless devices. With additional Summit WM-Series Switches, the number of wireless devices the system can support is in the thousands.
Integrates in existing network	A Summit WM-Series Switch can be added to an existing enterprise network as a new network device, greatly enhancing its capability without interfering with existing functionality. Integration of the Summit WM-Series Switches and Altitude APs does not require any reconfiguration of the existing infrastructure (e.g., VLANs).
Offers centralized management and control	An administrator accesses the Summit WM-Series Switch in its centralized location to monitor and administer the entire wireless network. The Summit WM-Series Switch has functionality to recognize, configure, and manage the Altitude APs and distribute new software releases.
Provides easy deployment of Altitude APs	The initial configuration of the Altitude APs on the centralized Summit WM-Series Switch can be done with an automatic “discovery” technique.
Provides security via user authentication	Summit WM-Series Switch Software uses existing authentication (AAA) servers to authenticate and authorize users.
Provides security via filters and privileges	Summit WM-Series Switch Software uses virtual networking techniques to create separate virtual networks with defined authentication and billing services, access policies and privileges.
Supports seamless mobility and roaming	Summit WM-Series Switch Software supports seamless roaming of a wireless device from one Altitude AP to another on the same Summit WM-Series Switch or on a different Summit WM-Series Switch.
Integrates third-party access points	Summit WM-Series Switch Software can integrate legacy third-party access points, using a combination of network routing and authentication techniques.
Prevents rogue devices	Unauthorized access points will be detected and identified as harmless or dangerous rogue APs.
Provides accounting services	Summit WM-Series Switch Software logs wireless user sessions, user group activity, and other activity reporting, enabling the generation of consolidated billing records.
Offers troubleshooting capability	Summit WM-Series Switch Software logs system and session activity and provides reports to aid in troubleshooting analysis.
Offers dynamic RF management	Summit WM-Series Switch Software can automatically select channels and adjust Radio Frequency (RF) signal propagation power levels without user intervention.

Summit WM-Series Switch Software and your network

Components of the solution: a summary

The following is a summary checklist of the components of the Summit WM-Series Switch Software solution on your enterprise network. These are described in detail in this guide.

- The **Summit WM-Series Switch**, providing centralized control over all access points (both Altitude APs and third-party access points) and manages the network assignment of wireless device clients associating through access points.
- The **Altitude AP** is a wireless LAN *thin access point* (IEEE 802.11) that communicates only with a Summit WM-Series Switch.
- **RADIUS Server** (Remote Access Dial-In User Service) (RFC2865), or other authentication server. Assigns and manages ID and Password protection throughout the network. Used for authentication of the wireless users in either 802.1x or Captive Port security modes.

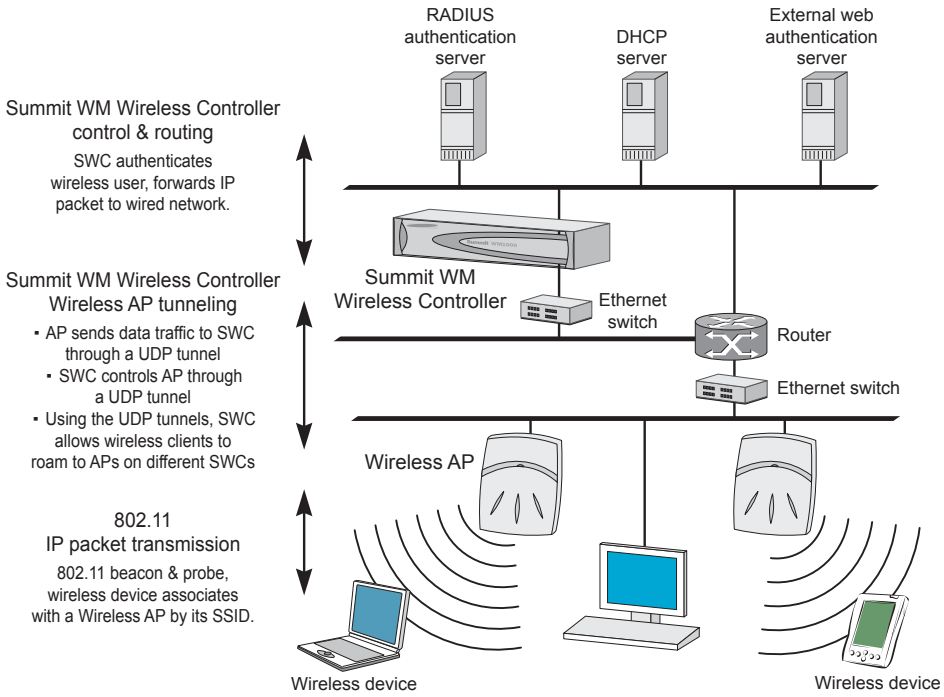
  The RADIUS Server system can be set up for certain standard attributes, such as Filter-ID, and for the Vendor Specific Attributes (VSAs).
- **DHCP Server** (Dynamic Host Configuration Protocol) (RFC2131). Assigns IP addresses, gateways and subnet masks dynamically. IP address assignment for clients can be done by the DCHP server internal to the Summit WM-Series Switch, or by existing servers using DHCP relay. Also used by the Altitude APs to discover the location of the Summit WM-Series Switch during the initial registration process. For SLP, DHCP should have Option 78 enabled (Option 78 specifies the location of one or more SLP Directory Agents).
- **Service Location Protocol (SLP)** (SLP RFC2608). Client applications are *User Agents* and services are advertised by *Service Agents*. In larger installations, a *Directory Agent* collects information from Service Agents and creates a central repository. The Extreme Networks solution relies on registering "extreme" as an SLP Service Agent.
- **Domain Name Server (DNS)**, for an alternate mechanism (if present on the enterprise network) for the automatic discovery process. Summit WM-Series Switch Software relies on the DNS for Layer 3 deployments and for static configuration of Altitude APs. The Extreme Networks solution relies on registering "controller" as the DNS name.
- **Web Authentication Server**, if desired for external authentication.
- **RADIUS Accounting Server** (Remote Access Dial-In User Service) (RFC2866), if RADIUS Accounting is enabled.
- **Simple Network Management Protocol** (SNMP) Manager Server, if forwarding SNMP messages is enabled.
- **Check Point Server**, Check Point Event Logging API (ELA), for security event logging if a firewall application is enabled.
- **Network infrastructure**, Ethernet switches and routers, must be configured to allow routing between the various services noted above.

  Routing must also be enabled between multiple Summit WM-Series Switches, for such Summit WM-Series Switch Software features as Availability, WM-AD Manager for mobility, Third-Party Access Points, and Summit Spy for detection of rogue access points (some features require the definition of static routes).
- **Web Browser**, providing access to the Summit WM-Series Switch Management GUI to configure Summit WM-Series Switch Software.

- a device that supports SSH, for serial port access to the Command Line Interface (CLI), for file management and monitoring by a network technician.

Network traffic flow

Figure 3: Traffic Flow diagram


RADIUS authentication server
DHCP server
External web authentication server
Summit WM Wireless Controller control & routing
SWC authenticates wireless user, forwards IP packet to wired network.
Summit WM Wireless Controller
Summit WM Wireless Controller Wireless AP tunneling
▪ AP sends data traffic to SWC through a UDP tunnel
▪ SWC controls AP through a UDP tunnel
▪ Using the UDP tunnels, SWC allows wireless clients to roam to APs on different SWCs
Ethernet switch
Router
Ethernet switch
Wireless AP
802.11 IP packet transmission
802.11 beacon & probe, wireless device associates with a Wireless AP by its SSID.
Wireless device
Wireless device

The diagram above shows a simple configuration with a single Summit WM-Series Switch and two Altitude APs, each supporting a wireless device. A RADIUS server on the network provides authentication, and a DHCP server is used by the Altitude APs to discover the location of the Summit WM-Series Switch during the initial registration process. Also present in the network are routers and ethernet switches.

Each wireless device sends IP packets in the 802.11 standard to the Altitude AP. The Altitude AP uses a UDP (User Datagram Protocol) based tunnelling protocol to encapsulate the packets and forward them to the Summit WM-Series Switch.

The Summit WM-Series Switch decapsulates the packets, and routes these to destinations on the network, after authentication by the RADIUS server.

The Summit WM-Series Switch functions like a standard router, except that it is configured to route only network traffic associated with wireless connected users. The Summit WM-Series Switch can also be configured to simply forward traffic to a default or static route if dynamic routing is not preferred.

Network security

The Summit WM-Series Switch Software system provides features and functionality to control network access. These are based on standard wireless network security practices.

Current wireless network security methods provide a degree of protection. These methods include:

- Shared Key authentication that relies on Wired Equivalent Privacy (WEP) keys
- Open System that relies on Service Set Identifiers (SSIDs)
- 802.1x that is compliant with Wi-Fi Protected Access (WPA)
- Captive Portal based on Secure Sockets Layer (SSL) protocol

The Summit WM-Series Switch Software system supports these encryption approaches:

- Wired Equivalent Privacy (WEP), a security protocol for wireless local area networks defined in the 802.11b standard
- Wi-Fi Protected Access version 1 (WPA1™) with Temporal Key Integrity Protocol (TKIP)
- Wi-Fi Protected Access version 2 (WPA2™) with Advanced Encryption Standard (AES) and Counter Mode with Chipher Block Chaining Message Authentication Code (CCMP).

Authentication

The Summit WM-Series Switch relies on a RADIUS server, or authentication server, on the enterprise network to provide the authentication information (whether the user is to be allowed or denied access to the network).

The Summit WM-Series Switch provides authentication using:

- Captive Portal, a browser-based mechanism that forces users to a web page
- RADIUS (using IEEE 802.1x)

The *802.1x mechanism* is a standard for authentication developed within the 802.11 standard. This mechanism is implemented at the port, blocking all data traffic between the wireless device and the network until authentication is complete. Authentication by 802.1x standard uses Extensible Authentication Protocol (EAP) for the message exchange between the Summit WM-Series Switch and the RADIUS server.

When 802.1x is used for authentication, the Summit WM-Series Switch provides the capability to dynamically assign per-wireless-device WEP keys (called per-station WEP keys in 802.11).

In Summit WM-Series Switch Software, a RADIUS redundancy feature is provided, where you can define a failover RADIUS server (up to 2 servers) in the event that the active RADIUS server fails.

Privacy

Privacy is a mechanism that protects data over wireless and wired networks, usually by encryption techniques.

Summit WM-Series Switch Software supports the Wired Equivalent Privacy (WEP) standard common to conventional access points.

It also provides Wi-Fi Protected Access version 1 (WPA v.1) encryption, based on Pairwise Master Key (PMK) and Temporal Key Integrity Protocol (TKIP). The most secure encryption mechanism is WPA version 2 using Advanced Encryption Standard (AES).

Interaction with wired networks: Wireless Mobility Access Domain

Summit WM-Series Switch Software provides a versatile means of mapping wireless networks to the topology of an existing wired network. This is accomplished through the assignment of *WM Access Domain Services*.

When you set up WM Access Domain Services (WM-AD) on the Summit WM-Series Switch, you are defining subnets for groups of wireless users. This WM-AD definition creates a virtual IP subnet where the Summit WM-Series Switch acts as a default gateway for wireless devices.

This technique enables policies and authentication to be applied to the groups of wireless users on a WM-AD, as well as the collecting of accounting information on user sessions that can be used for billing.

When a WM-AD is set up on the Summit WM-Series Switch:

- one or more Altitude APs (by radio) are associated with it
- a range of IP addresses is set aside for the Summit WM-Series Switch's DHCP server to assign to wireless devices

If routing protocol is enabled, the Summit WM-Series Switch advertises the WM-AD as a routable network segment to the wired network, and routes traffic between the wireless devices and the wired network.

Each radio on a Altitude AP can participate in up to four WM-ADs, via the multi-SSID function.

Static routing and routing protocols

Routing can be used on the Summit WM-Series Switch to support the WM-AD definitions.

In the User Interface, you can configure routing on the Summit WM-Series Switch to use one of the following routing techniques:

- Static routes: Use static routes to set the default route of a Summit WM-Series Switch so that legitimate wireless device traffic can be forwarded to the default gateway.
- Open Shortest Path First (OSPF, version 2) (RFC2328): Use OSPF to specify the next best hop (route) of a Summit WM-Series Switch. Open Shortest Path First (OSPF) is a protocol designed for medium and large IP networks, with the ability to segment routers into different routing areas for routing information summarization and propagation.
- Next Hop Routing: Use next hop routing as part of a WM-AD definition to specify a unique default gateway to which traffic on a unique WM-AD is forwarded.

Policy: packet filtering

Policy refers to the rules that allow different network access to different groups of users. The Summit WM-Series Switch Software system can link authorized users to user groups. These user groups then can be confined to predefined portions of the network.

In the Summit WM-Series Switch Software system, policy is carried out by means of packet filtering, within a WM-AD.

In the Summit WM-Series Switch user interface, you set up a filtering policy by defining a set of hierarchical rules that allow (or deny) traffic to specific IP addresses, IP address ranges, or services (ports). The sequence and hierarchy of these filtering rules must be carefully designed, based on your enterprise's user access plan.

The authentication technique selected determines how filtering is carried out:

- If authentication is by SSID and Captive Portal, a non-authenticated filter will allow all users to get as far as the Captive Portal web page, where login occurs. When authentication is returned, then filters are applied, based on user ID and permissions.
- If authentication is by AAA (802.1x), users will already have logged in and have been authenticated before being assigned an IP address. At this point, filters are applied, based on user ID and permissions.

Mobility and roaming

The 802.11 standard allows a wireless device to preserve its IP connection when it roams from one access point to another on the same subnet. However, if a user roams to an access point on a different subnet, the user is disconnected.

Summit WM-Series Switch Software has functionality that supports mobility on any subnet in the network. Wireless device users can roam between Altitude APs on any subnet without having to renew the IP connection.

The Summit WM-Series Switch stores the wireless device's current session information, such as IP address and MAC address. If the wireless device has not disassociated, then when it requests network access on a different Altitude AP, the Summit WM-Series Switch can match its session information and recognize it as still in a current session.

In addition, a Summit WM-Series Switch can learn about other Summit WM-Series Switches on the network, and then exchange client session information. This enables a wireless device user to roam seamlessly between different Altitude APs on different Summit WM-Series Switches.

Availability

Summit WM-Series Switch Software provides seamless availability against Altitude AP outages, Summit WM-Series Switch outages, and even network outages.

For example, if one Altitude AP fails, coverage for the wireless device is automatically provided by the next nearest Altitude AP.

If a Summit WM-Series Switch fails, all of its associated Altitude APs, or access points, can automatically migrate to another Summit WM-Series Switch that has been defined as the secondary or backup Summit WM-Series Switch. When the original Summit WM-Series Switch returns to the network, the Altitude APs automatically re-establish their normal connection with their original Summit WM-Series Switch.

Quality of Service (QoS)

Summit WM-Series Switch Software provides advanced Quality of Service (QoS) management, in order to provide better network traffic flow. Such techniques include:

- WMM (Wi-Fi Multimedia): enabled globally on the Altitude AP. For devices with WMM enabled., the standard provides multimedia enhancements for audio, video, and voice applications. WMM shortens the time between transmitting packets for higher priority traffic. WMM is part of the 802.11e standard for QoS.
- IP ToS (Type of Service) or DSCP (Diffserv Codepoint): the ToS/DSCP field in the IP header of a frame is used to indicate the priority and Quality of Service for each frame. The IP TOS and/or DSCP is maintained within CTP (CAPWAP Tunneling Protocol) by copying the user IP QoS information to the CTP header — this is referred to as Adaptive QoS.

Quality of Service (QoS) management is also provided by:

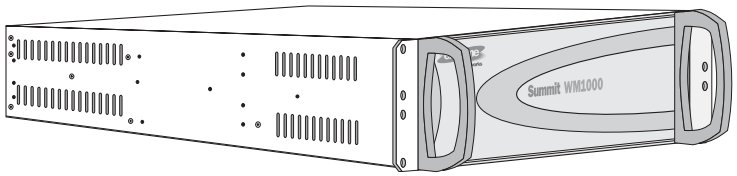
- assigning high priority to an SSID (configurable)
- Adaptive QoS (automatic)
- support for legacy devices that use SpectraLink Voice Protocol (SVP) for prioritizing voice traffic (configurable)

2 Summit WM-Series Switch: Startup

Summit WM-Series Switch features and installation

The Summit WM-Series Switch is a network device designed to be integrated into an existing wired Local Area Network (LAN).

Figure 4: The Summit WM-Series Switch



The Summit WM-Series Switch provides centralized management, network access and routing to wireless devices that are using Altitude APs to access the network. It can also be configured to handle data traffic from third-party access points.

The Summit WM-Series Switch performs the following functions:

- Controls and configures Altitude APs, providing centralized management
- Authenticates wireless devices that contact a Altitude AP
- Assigns each wireless device to a WM-AD when it connects
- Routes traffic from wireless devices, using WM-ADs, to the wired network
- Applies filtering policies to the wireless device session
- Provides session logging and accounting capability

The Summit WM-Series Switch is rack-mountable. It comes in the following product families:

Model Number	Specifications
Summit WM-Series Switch Summit WM100	• Four Fast-Ethernet ports, (10/100 BaseT), supporting up to 75 Altitude APs • One management port, (10/100 BaseT) • One console port (DB9 serial) • Power supply redundant (R)
Summit WM-Series Switch Summit WM1000	• Two GigE ports (dual 1GB SX network interfaces), supporting up to 200 Altitude APs • One management port, (10/100 BaseT) • One console port (DB9 serial) • Power supply redundant (R)

Installing the Summit WM-Series Switch

Before you begin installation, make sure that a site survey has been done, to determine the number and location of Altitude APs and Summit WM-Series Switches required. The site survey should take a number of factors into consideration, including:

- coverage areas
- number of users
- architectural features that affect transmission
- existing wired network and access to ethernet cabling
- type of mount (wall, ceiling, plenum) for Altitude APs
- type of power (Power-over-Ethernet or AC adaptor) for Altitude APs
- physical security of the Summit WM-Series Switch, including access control

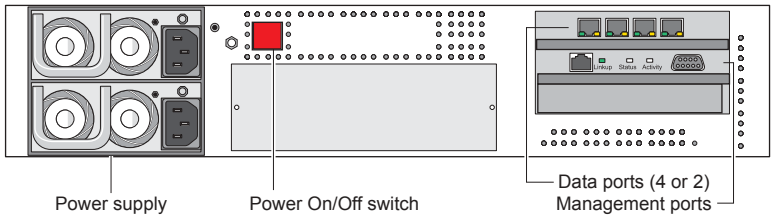
Installing the Summit WM-Series Switch

1 Unpack and mount the Summit WM-Series Switch following the detailed instructions in the Quick Start Guide

2 Install the ferrite beads provided, black for the power cord and white for the ethernet cables, as described in the *Quick Start Guide*.

3 Plug the Summit WM-Series Switch power supply (single or dual) in to the back of the Controller.

Figure 5: The Summit WM-Series Switch – back view diagram



4 Perform initial setup of the Summit WM-Series Switch to change its factory default IP address.

5 After that, connect the Summit WM-Series Switch to the enterprise LAN.

First-time setup of Summit WM-Series Switch

Management port first-time setup

Before you can connect the Summit WM-Series Switch to the enterprise network, you must change the IP address of the Summit WM-Series Switch management port from its factory default to the IP address suitable for your enterprise network.

Access the Summit WM-Series Switch for initial setup by one of two methods:

- a device supporting VT100 emulation such as a PC running HyperTerm, attached to the Summit WM-Series Switch's DB9 serial port (COM1 port) via a cross-over (null modem) cable. The

Command Line Interface (CLI) commands for the initial setup are described in an attached appendix.

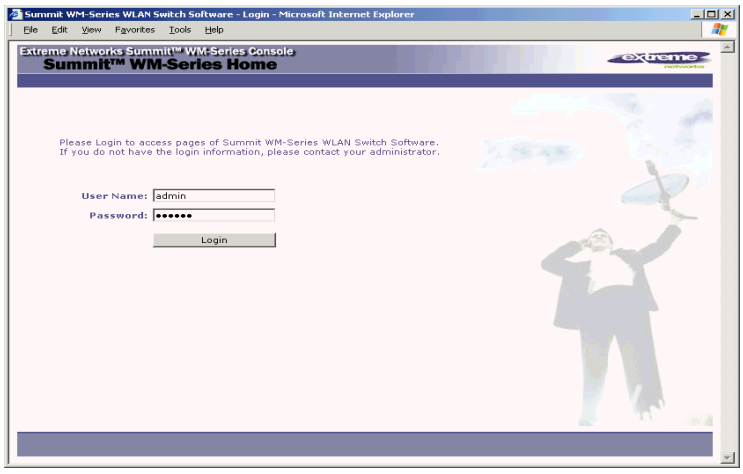
- a laptop computer, running a web browser such as Internet Explorer 6.0 (or higher), attached to the Summit WM-Series Switch's ethernet Management Port (RJ45 port) via an ethernet cross-over cable (cable provided with the Summit WM-Series Switch). The steps for initial setup in the Graphical User Interface are described below.

The factory default management port setup of the Summit WM-Series Switch is:

Hostname:	**SWM**
Management Port IP address:	192.168.10.1:5825
Management Network Mask:	255.255.255.0

Changing the Management Port IP address: web browser method

1. Connect a cross-over ethernet cable between the ethernet port of the laptop and ethernet Management Port of the Summit WM-Series Switch.
2. Statically assign an unused IP address in the 192.168.10.0/24 subnet for the ethernet port of the PC (for example, 192.168.10.205).
3. Run Internet Explorer (version 6.0 or above) or other web browser on the laptop.
4. Point the browser to the URL https://192.168.10.1:5825. This URL launches the web-based GUI on the Summit WM-Series Switch. The login screen appears.

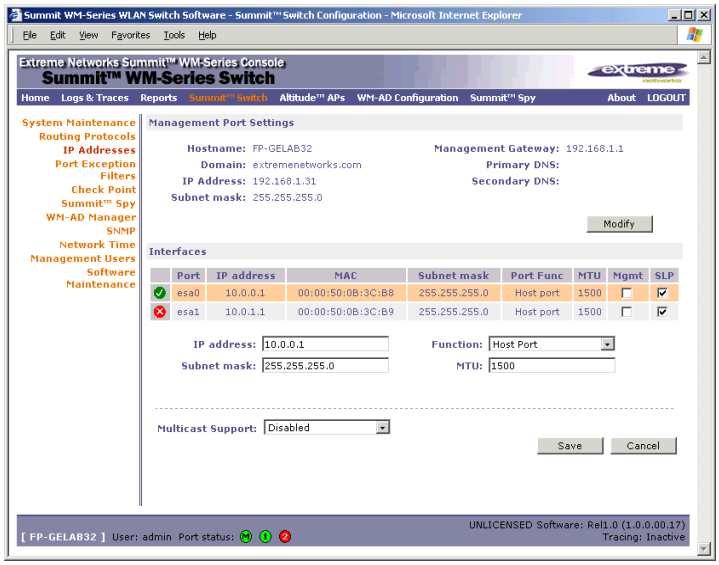

Summit WM-Series WLAN Switch Software - Login - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Extreme Networks Summit™ WM-Series Console
Summit™ WM-Series Home
Please Login to access pages of Summit WM-Series WLAN Switch Software.
If you do not have the login information, please contact your administrator.
User Name: admin
Password:
Login

5 Key in the factory default **User Name** (“admin”) and **Password** (“abc123”). Click on the **Login** button. The main menu screen appears.

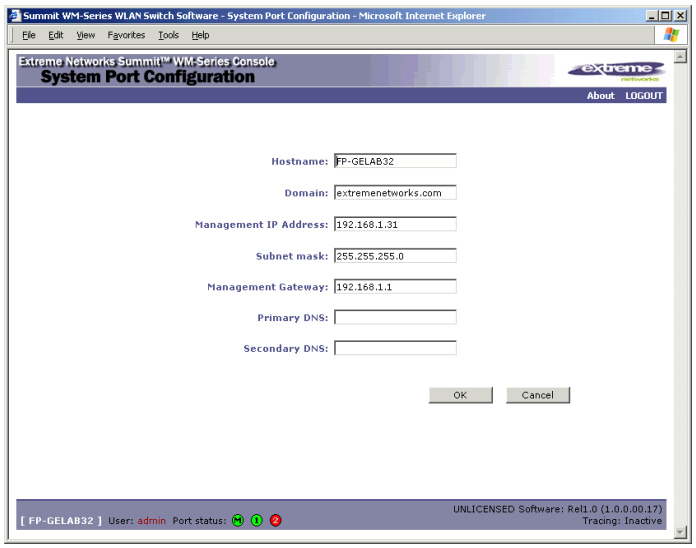
Summit WM-Series WLAN Switch Software - Web Client Home - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Extreme Networks Summit™ WM-Series Console
Summit™ WM-Series Home
About LOGOUT
Logs & Traces
Reports & Displays
Summit™ Switch Configuration
Altitude™ AP Configuration
WM Access Domain Configuration
Summit™ Spy
UNLICENSED Software: Rel1.0 (1.0.0.00.17)
Tracing: Inactive
[FP-GELAB32] User: admin Port status:

6 Click on the Summit WM-Series Switch Configuration menu option to navigate to the *Summit WM-Series Switch Configuration* screen.

7 In the left-hand list, click on the **IP Addresses** option. The Management Port Settings area (top portion of the screen) displays the factory settings for the Summit WM-Series Switch.



8 To modify Management Port Settings, click the **Modify** button. The *System Port Configuration* screen appears.



9 Key in:

Hostname	The name of the Summit WM-Series Switch
Domain	The IP domain name of the enterprise network
Management IP Address	The new IP address for the Summit WM-Series Switch's management port (change this as appropriate to the enterprise network).
Subnet mask	For the IP address, the appropriate subnet mask to separate the network portion from the host portion of the address (typically 255.255.255.0)
Management Gateway	The default gateway of the network.
Primary DNS	The primary name server used by the network.
Secondary DNS	The secondary name server used by the network

10 Click **OK** to return to the *Summit WM-Series Switch Configuration* screen.

11 Click on the Save button to save the port changes.

The web connection between the laptop and the Summit WM-Series Switch is now lost, because their IP addresses are now on different networks.

Adding the Summit WM-Series Switch to your enterprise network

1 Disconnect the laptop from the Summit WM-Series Switch Management Port.

2 Connect the Summit WM-Series Switch Management Port to the enterprise ethernet LAN.

The Summit WM-Series Switch resets automatically. Now you will be able to launch the Summit WM-Series Switch Software GUI again, with the system visible to the enterprise network.

The remaining steps in initial configuration of the Summit WM-Series Switch Software system are described in the next topic, after an overview of the GUI.

The graphical user interface (GUI): overview

The administrator can configure and administer the Summit WM-Series Switch Software system using the web-based Graphical User Interface.

To run the graphical user interface

1 Launch Microsoft Internet Explorer (version 6.0 or above), or other web browser.

2 In the address bar, key in the URL https://x.x.x.x:5825 (your management gateway as defined in initial setup plus port 5825, formerly factory default 192.168.10.1:5825). The Summit WM-Series Switch Software login screen appears.

3 Key in the factory default **User Name** ("admin") and **Password** ("abc123"). Click on the **Login** button. The main menu screen appears.

NOTE

You can define which user names have full read/write access to the user interface ("Admin" users) and which users have "read-only" privileges. This is done the Summit WM-Series Switch Configuration: Management Users screen.

The main areas in the Summit WM-Series Switch Software user interface are accessed from the main menu, or by clicking on the appropriate tab across the top of each screen. Within each area, to access the associated subscreens, click on the screen name in the left-hand list.

Table 2: Summit WM-Series Switch Software user interface summary

Tab	Screen	Function
Logs & Traces		Logs normal events and alarm events Trace logs are by component.
Reports & Displays		Access to various on-screen reports
Summit WM-Series Switch Configuration	System Maintenance Routing Protocols IP Addresses Check Point Summit Spy WM-AD Manager SNMP Network Time Management Users Software Maintenance	Tasks including shutdown, enable syslog. Define static routes, configure OSPF. Set up management port (Modify screen) Set up the data ports. Enable event logging for Check Point. Enable "detect rogue APs" mechanism. Manage multiple Summit WM-Series Switches. Enable SNMP messages to be sent. Configure synchronized time. Define user level. Product Keys and software upgrades.
Altitude AP Configuration	Highlight a AP Access Approval AP Maintenance AP Registration Client Disassociate	Modify properties, radios, static config. Modify the status of a Altitude AP. View and set up AP software upgrade. Define registration mode, pairing of APs. Force a wireless device to disassociate.

Table 2: Summit WM-Series Switch Software user interface summary (Continued)

Tab	Screen	Function
WM-AD Configuration	Global Settings	Define RADIUS servers,& global settings
	Add a subnet	Left-hand list. Enter name. Click to add.
	WM-AD Topology	Define the WM-AD topology, authentication and accounting set up
	WM-AD Authen & Acct	
	WM-AD RADIUS Policy	Define Filter IDs
	WM-AD Filtering	Define filtering rules to control access
	WM-AD Privacy	Set up WEP keys or WPA privacy.
Summit Spy		Configure and view reports for the Summit Spy (rogue access point detection)

3 Summit WM-Series Switch Software configuration

Configuration steps: overview

To set up and configure the Summit WM-Series Switch and Altitude APs, follow these steps:

1. *First-time Setup*: Perform "First-Time Setup" of the Summit WM-Series Switch on the physical network to modify the Management Port IP address for the enterprise network.
2. *Product Key*: Apply a Product Key file, for licensing purposes.
3. *Data Port Setup*: Set up the Summit WM-Series Switch on the network by configuring the physical data ports and their function as "host port", "router port", or "3rd party AP port".
4. *Routing Setup*: For any port defined as a "router port", configure static routes and OSPF parameters, if appropriate to the network
5. *Altitude AP Initial Setup*: Connect the Altitude APs to the Summit WM-Series Switch. They will automatically begin the "Discovery" of the Summit WM-Series Switch, based on factors that include:
   - their Registration mode (in the *Altitude AP Registration* screen)
   - the enterprise network services that will support the discovery process.
6. *Altitude AP Configuration*: Modify properties or settings of the Altitude AP, if desired.
7. *WM Access Domain Services Setup*: Set up one or more virtual subnetworks on the Summit WM-Series Switch. For each WM-AD, configure the following:
   - Topology: configure the WM-AD, and assign the Altitude APs radios to the WM-AD.
   - Authentication and Accounting: configure the authentication method for the wireless device user and enable the accounting method.
   - RADIUS Policy: define Filter ID values for user groups
   - Filtering: define filtering rules to control network access
   - Multicast: define groups of IP addresses for multicast traffic
   - Privacy: select and configure the wireless security method on the WM-AD.

Enabling the product key

Once the "First-Time Setup" is complete, the next step in the initial setup of the Summit WM-Series Switch is to enter your product key. This is a one-time event. The Product Key file is provided with your Summit WM-Series Switch in a downloaded file.

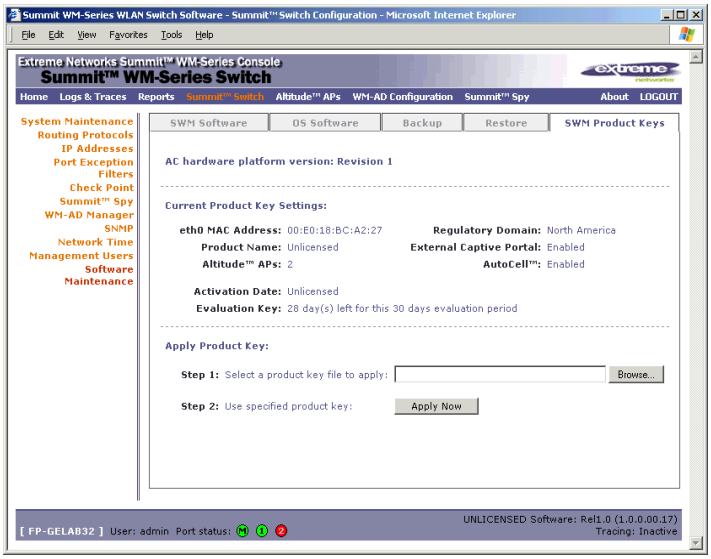
For assistance, if you cannot find the product key, contact your local representative. To find your nearest service organization, access the Extreme Networks website at www.extremenetworks.com, and then select your country's Extreme website from the drop-down list. The service organizations for your country will be listed on the local site. This product area is IP Convergence Solutions or Wireless.

If no Product Key is enabled, the Summit WM-Series Switch functions with all features enabled in demonstration mode.

Enabling the product key on the Summit WM-Series Switch

1 Click on the **Summit Switch** tab. The *Summit WM-Series Switch Configuration* screen appears. Click on the **Software Maintenance** option. Then click on the **SWM Product Keys** tab. The *Product Keys* screen appears.

The top portion of the screen displays the current Product Key settings. The lower portion permits you to browse for a Product Key file and apply it.



2 To select a product key file, click **Browse** to navigate to a downloads folder or a CD drive.

3 To activate this product key file, click **Apply Now**.

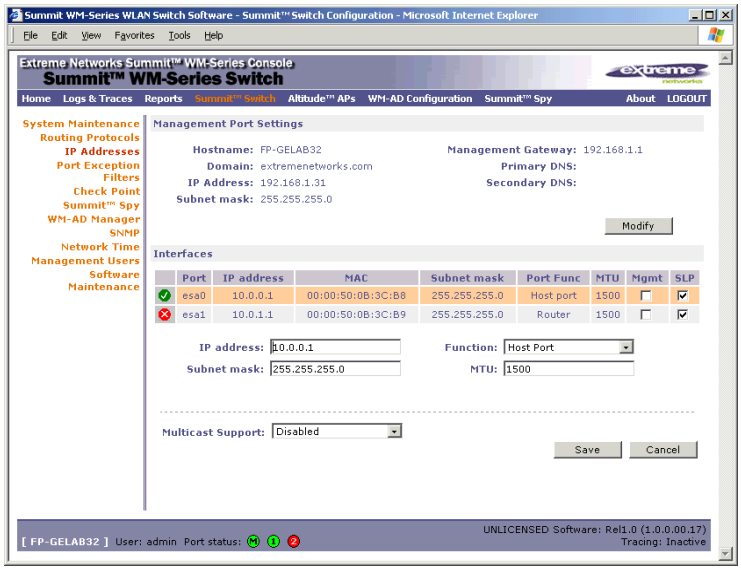
Setting up the data ports

The next step in the initial setup of the Summit WM-Series Switch is to configure the physical data ports.

Configuring the data port interfaces on the Summit WM-Series Switch

1 Click on the **Summit Switch** tab. In the *Summit WM-Series Switch Configuration* screen, click on the **IP Address** option. The *Management Port Settings and Interfaces* screen appears.

The lower portion of the *Summit WM-Series Switch Configuration* screen displays the **Interfaces**, either the four ethernet ports (for the Summit WM100 and Summit WM1000), or the two ports (for the Summit WM1000). For each port, the MAC address is displayed automatically.



2 Click in a port row to highlight it.

3 For the highlighted port, key in the:

IP address	IP Address of the physical ethernet port.
Subnet mask	For the IP address, the appropriate subnet mask to separate the network portion from the host portion of the address (typically 255.255.255.0)
MTU	Maximum Transmission Unit (maximum packet size for this port). Default setting is 1500. If you change this setting, and are using OSPF, be sure that the MTU of each port in the OSPF link matches.

NOTE

In a "Branch Office" scenario, where the Altitude AP is configured statically on a local network whose MTU is lower than 1500, the Summit WM-Series Switch automatically adjusts the MTU size to prevent packet fragmentation.

4 For the highlighted port, select its **Function** from the drop-down list: Host Port, 3rd Party AP, Router (defined below).

For OSPF routing on a port, that port must be configured as a "Router" Port. No more than one port should be configured as a router port.

5 To allow Management traffic on a highlighted port, click the **Mgmt** checkbox on. This choice must be used carefully since it overrides the built-in protection filters on the port.

6 For the highlighted port, click the **SLP** checkbox on to allow SLP protocol on this port for Altitude APs using this port for discovery and registration.

7 To save the port configuration, click **Save**.

To cancel the entries without saving, click **Cancel**.

Port Type or Function

A new Summit WM-Series Switch is shipped from the factory with all its data ports set up as "Host ports", and support of management traffic disabled on all data ports. In the *Summit WM-Series Switch Configuration – IP Addresses* screen, you can redefine the data ports to function as one of three types:

- Host Port

  Use "Host Port" for connecting Altitude APs, with no dynamic routing. A "Host Port" has dynamic routing disabled to ensure that the port does not participate in dynamic routing operations, such as OSPF, to advertise the availability of WM-ADs hosted by the Summit WM-Series Switch. "Host Ports" may still be used as the target for static route definitions.

- Third-Party AP Port

  Define as "3rd-Party AP" a port to which you will connect third-party access points. No more than one port can be configured for third-party APs.

  Selecting this option prepares the port to support a third-party AP setup that allows the mapping of an WM-AD to the physical port. The WM-AD settings then permit the definition of policy, such as filters and Captive Portal, that manage the traffic flow for wireless users connected to these access points.

  The third-party access points must be operating as layer-2 bridges. The "third-party AP" WM-AD is isolated from the rest of the network. The Summit WM-Series Switch assumes control over the layer-3 functions such as DHCP.

  Altitude APs must not be attached to a "3rd-Party AP" port.

- Router Port

  Define as "Router Port" a port that you wish to connect to an upstream next-hop router in the network. Dynamic routing protocol such as OSPF can be turned on for this port type.

  Altitude APs can be attached to a "Router" port. The Summit WM-Series Switch will create a virtual WM-AD port and handle wireless device traffic in the same manner as a "Host port". Third-party access points must not be directly connected to a "Router" port.

There is a fourth port type that is not configurable in the user interface:

- WM Access Domain Services (WM-AD) interface

  An WM-AD port is a virtual port created automatically on the Summit WM-Series Switch when a new WM-AD is defined. The WM-AD port becomes the default gateway for wireless devices on this WM-AD. No Altitude APs can be associated with an WM-AD port and no routing is permitted on this port.

The chart below summarizes the port types and their functions:

Table 3: Port types and functions

Port Type	IP Forwarding	Altitude AP support	Mgmt traffic support (SNMP, HTTP, TELNET, SLP, RADIUS, DHCP)	Routing protocol support (IP, OSPF and PIM)
Host	No	Yes	Selectable	No
3rd-Party AP	No	No	Selectable	No
Router	Selectable. Route wireless device traffic only	Yes	Selectable	Selectable
WM-AD	No	No	Selectable	No

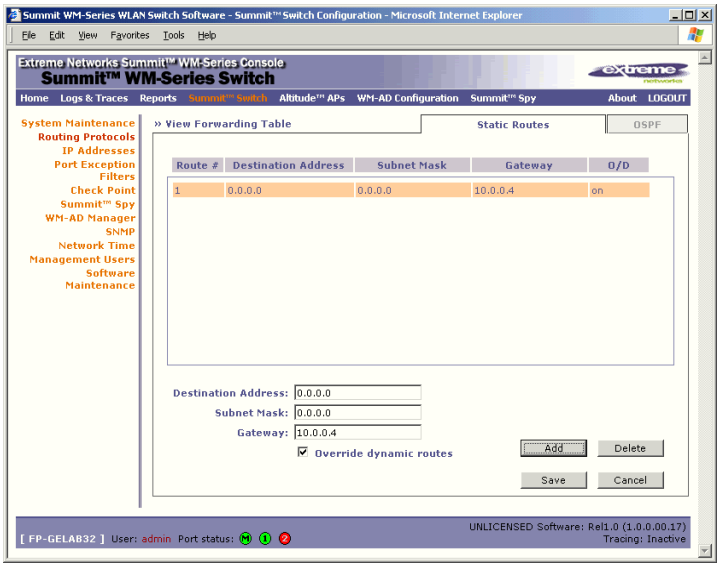
Setting up static routes

It is recommended that you define a default route to your enterprise network, either with a static route or by using OSPF protocol. This will enable the Summit WM-Series Switch to forward wireless packets to the remainder of the network.

Setting up a static route on the Summit WM-Series Switch

1 Click on the **Summit Switch** tab. In the *Summit WM-Series Switch Configuration* screen, click on the **Routing Protocols** option.

2 Click the **Static Routes** tab. The *Static Routes* screen appears.



3 To add a new route, click in the Destination Address field and key in the destination IP address of a packet.

[The destination network IP address that this static route applies to. Packets with this destination address will be sent to the Destination below.]

To define a *default static route* for any unknown address not in the routing table, key in 0.0.0.0.

4 Key in the Subnet Mask. For the IP address, the appropriate subnet mask to separate the network portion from the host portion of the address (typically 255.255.255.0).

For the *default static route* for any unknown address, key in 0.0.0.0.

5 In the **Gateway** field, key in the IP address of the gateway (the IP address of the specific router port or gateway on the same subnet as the Summit WM-Series Switch to which to route these packets; that is, the IP address of the next hop between the Summit WM-Series Switch and the packet's ultimate destination).

6 Click on the **Add** button. The new route appears in the list, numbered sequentially.

7 The **Override dynamic routes** checkbox is *on* by default. This means the static routes defined here will have priority over the OSPF learned routes (including default route) that the Summit WM-Series Switch uses for routing. If you wish to remove this priority for static routes, so that routing is controlled dynamically at all times, click the **Override dynamic routes** checkbox *off*.

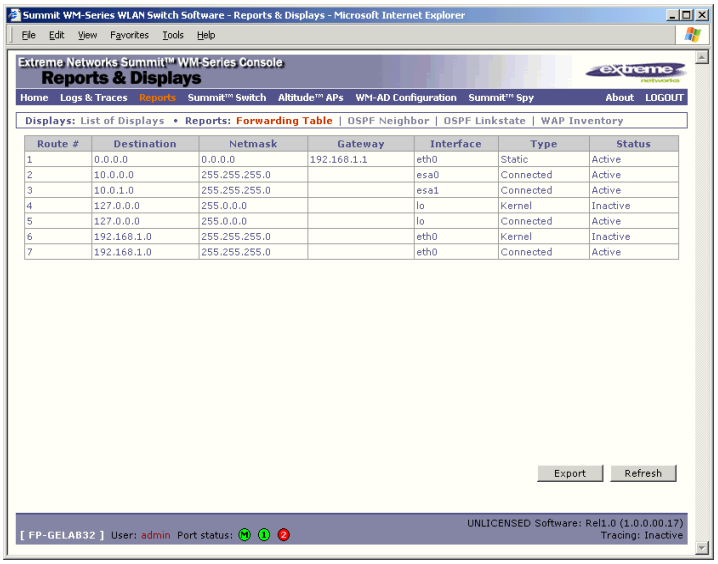
NOTE

If you enable dynamic routing (OSPF), the dynamic routes will normally have priority for outgoing routing. For internal routing on the Summit WM-Series Switch, the static routes normally have priority.

8 Click on **Save** to update the routing table on the Summit WM-Series Switch.

Viewing the Routing Table on the Summit WM-Series Switch

To view the static routes that have been defined for the Summit WM-Series Switch, click on the **View Forwarding Table** tab. This displays the *Forwarding Table* also accessed in the **Reports & Displays** area of the user interface.


Summit WM-Series WLAN Switch Software - Reports & Displays - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Extreme Networks Summit™ WM-Series Console
Reports & Displays
Home Logs & Traces Reports Summit™ Switch Altitude™ APs WM-AD Configuration Summit™ Spy About LOGOUT
Displays: List of Displays • Reports: Forwarding Table | OSPF Neighbor | OSPF Linkstate | WAP Inventory
Route # Destination Netmask Gateway Interface Type Status
1 0.0.0.0 0.0.0.0 192.168.1.1 eth0 Static Active
2 10.0.0.0 255.255.255.0 esa0 Connected Active
3 10.0.1.0 255.255.255.0 esa1 Connected Active
4 127.0.0.0 255.0.0.0 lo Kernel Inactive
5 127.0.0.0 255.0.0.0 lo Connected Active
6 192.168.1.0 255.255.255.0 eth0 Kernel Inactive
7 192.168.1.0 255.255.255.0 eth0 Connected Active
Export
Refresh
[FP-GELAB32] User: admin Port status:
UNLICENSED Software: Rel1.0 (1.0.0.00.17)
Tracing: Inactive

This report displays all defined routes, whether static or OSPF, and their current status. To update the display, click on the **Refresh** button.

Setting up OSPF Routing

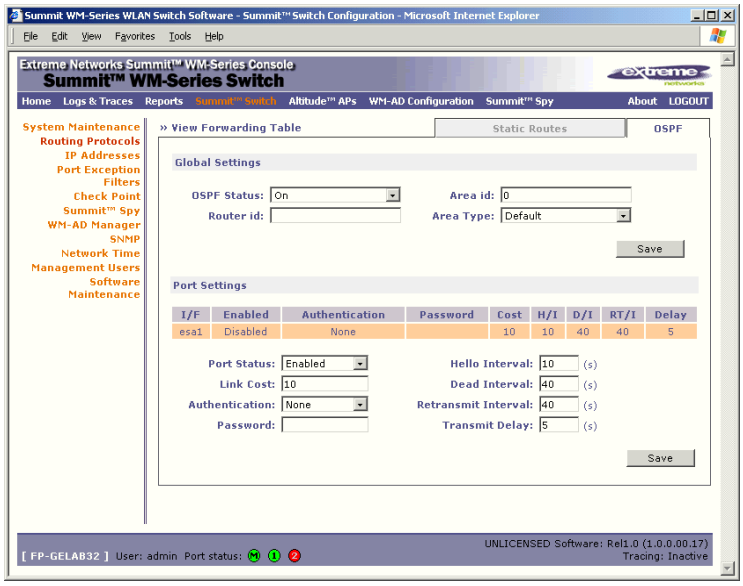
To enable OSPF routing, you must first define one data port as a "Router Port" in the *IP Addresses* screen. Next, enable OSPF globally on the Summit WM-Series Switch, and define the global OSPF parameters. Then you enable (or disable) OSPF on the port that you defined as a "Router Port".

Ensure that the OSPF parameters defined here for the Summit WM-Series Switch are consistent with the adjacent routers in the OSPF area. The parameters include the following:

- If the peer router has different timer settings, the protocol timer settings in the Summit WM-Series Switch must be changed to match, in order to achieve OSPF adjacency.
- The MTU of the ports on either end of an OSPF link must match. The MTU for ports on the Summit WM-Series Switch is defined as 1500, in the IP Addresses screen, during data port setup. This matches the default MTU in standard routers.

Setting up OSPF Routing on the Summit WM-Series Switch

1 Click on the OSPF tab in the *Routing Protocols* screen. The *OSPF Settings* screen appears.



2 In the Global Settings area, enable OSPF by filling in the following fields:

OSPF Status:	To enable OSPF, select ON from the drop-down list.
Router ID:	If left blank, the OSPF daemon will automatically pick a router ID from one of the Summit WM-Series Switch's interface IP addresses. If filled in here with the IP address of the Summit WM-Series Switch, this ID must be unique across the OSPF area.
Area ID:	0 is the main area in OSPF
Area Type:	Select Default (Normal), Stub, or Not-so-stubby (OSPF area types) from the drop-down list.

3 To save these settings, click on the **Save** button.

4 In the Port Settings area, for the data port defined as a "Router Port", fill in these fields:

Port Status:	To enable OSPF on the port, select Enabled from the drop-down list.
Link Cost:	Key in the OSPF standard for your network for this port. Default displayed is 10. (The cost of sending a data packet on the interface. The lower the cost, the more likely the interface is to be used to forward data traffic.)

NOTE

If more than one port is enabled for OSPF, it is desirable to prevent the Summit WM-Series Switch from serving as a router for other network traffic (other than the traffic from wireless device users controlled by the Summit WM-Series Switch). To ensure that the Summit WM-Series Switch is never the preferred OSPF route, one solution is to set the Link Cost to its maximum value of 65535. Filters should also be defined in the WM Access Domain Configuration – Filtering screen that will drop routed packets.

Authentication:	From the drop-down list, select the authentication type set up for the OSPF on your network: **None** or **Password**.
Password:	If "Password" was selected above, key it in here. This password must match on either end of the OSPF connection.
Dead-Interval:	Time in seconds (displays OSPF default).
Hello-Interval:	Time in seconds (displays OSPF default).
Retransmit-Interval:	Time in seconds (displays OSPF default).
Transmit delay:	Time in seconds (displays OSPF default).

5 To save these settings, click on the **Save** button.

To confirm that the ports are set up for OSPF, and that advertised routes from the upstream router are recognized, click View Forwarding Table to view the Forwarding Table report. Two additional reports display OSPF information when the protocol is in operation:

- *OSPF Neighbor* report displays the current neighbors for OSPF (routers that have interfaces to a common network)
- *OSPF Linkstate report* shows the Link State Advertisements (LSAs) received by the currently running OSPF process. The LSAs describe the local state of a router or network, including the state of the router's interfaces and adjacencies.

Filtering at the interface level

The Summit WM-Series Switch Software has a number of built-in filters that protect the system from unauthorized traffic. These filters are applied at the network interface level and are automatically invoked.

In addition to these built-in filters, the administrator can define specific exception filters at the interface-level to customize network access. These filters do not depend on a WM-AD definition.

Port-based exception filters: built-in

On the Summit WM-Series Switch, various port-based exception filters are built in and invoked automatically. These filters protect the Summit WM-Series Switch from unauthorized access to system management functions and services via the ports.

For example, on the Summit WM-Series Switch's data interfaces (both physical interfaces and WM-AD virtual interfaces), the built-in exception filter prohibits invoking SSH, HTTPS, or SNMP. However, such traffic is allowed, by default, on the Management port.

To enable SSH, HTTPS, or SNMP access through a data interface, select the interface in the *IP Addresses* screen and click the "Management" checkbox on. You can also enable such management traffic in the WM-AD definition.

If management traffic is explicitly enabled for any interface (physical port or WM-AD), access is implicitly extended to that interface through any of the other interface. (WM-AD).

Only traffic specifically allowed by the interface's exception filter is allowed to reach the Summit WM-Series Switch itself. All other traffic is dropped. Exception filters are dynamically configured, and are regenerated whenever the system's interface topology changes (a change of IP address for any interface).

Enabling management traffic on an interface adds additional rules to the exception filter to open up the well-known IP(TCP/UDP) ports corresponding to the HTTPS, SSH and SNMP applications.

The port-based built-in exception filtering rules, in the case of traffic from WM-AD users, operate only on traffic that is targeted directly to one of the WM-AD's interfaces. For example, a WM-AD filter may be generic enough to allow traffic access to the Summit WM-Series Switch's management (Allow All [*.*.*.*]). The traffic will initially be allowed according to the WM-AD user's policy, but may then be denied by the exception filter of the WM-AD interface.

Port-based exception filters: user defined

You can add specific filtering rules at the port level in addition to the built-in rules. Such rules give you the capability of restricting access to a port, for specific reasons, such as a Denial of Service (DoS) attack.

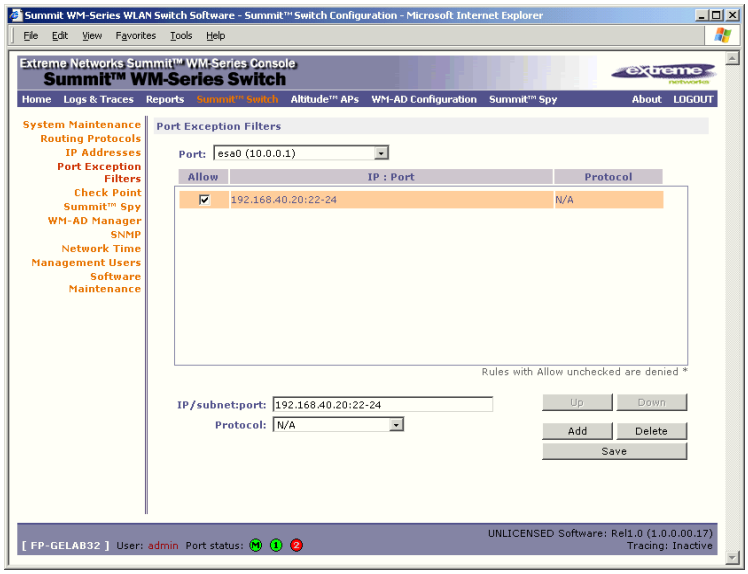
To define filtering rules that are associated with one of the physical data ports on the Summit WM-Series Switch rather than with a WM-AD, use the *Port Exception Filter* screen.

The filtering rules are set up in the same manner as filtering rules defined for a WM-AD — specify an IP address and then either "Allow" or "Deny" traffic to that address. See "Filtering rules for a WM-AD" on page 86.

Exception filtering rules that you will define for a WM-AD will apply to the wireless device users after their authentication, whereas the filtering rules that you define here apply to all traffic on a physical port.

Define port exception filters

1 Click on the **Summit Switch** tab. Click on the **Port Exception Filters** option. The *Port Exception Filters* screen appears.



2 Select the data port from the pull-down list to which these filters will apply.

3 For each filtering rule you are defining:

IP / Port: Type in the destination IP address. You can also specify an IP range, a port designation or a port range on that IP address.

Protocol: Default is N/A. To specify a protocol, select from the drop-down list (may include UDP, TCP, IPsec-ESP, IPsec-AH, ICMP).

4 Click on the **Add** button. The information appears in a new line in the **Filter** area of the screen.

5 Highlight the new filtering rule and click **Allow** checkbox *on* to *allow traffic.* Leave unchecked to *disallow traffic.*

6 Edit the order of a filtering rule by highlighting the line and clicking on the **Up** and **Down** buttons. The filtering rules are executed in the order defined here.

7 To save the filtering rules, click on the **Save** button.

4 Altitude AP: startup

You are now ready to add the Altitude APs to the Summit WM-Series Switch Software system and register them with the Summit WM-Series Switch. Before the Altitude APs can handle wireless traffic, you will also need to assign the Altitude APs to a WM-AD.

NOTE

Changes or modifications made to the Summit WM-Series Switch or the Altitude APs which are not expressly approved by Extreme and/or the party responsible for compliance upon installation could void the user's authority to operate the equipment.

Altitude AP features

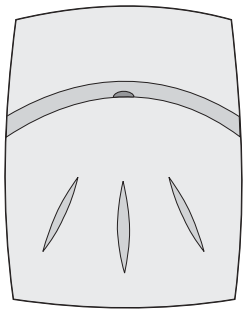
The Altitude AP is a wireless LAN access point using the 802.11 wireless standards (802.11a, 802.11b and 802.11g) for network communications. The Altitude AP bridges network traffic to an Ethernet LAN.

The Altitude AP is provided with proprietary software that allows it to communicate only with the Summit WM-Series Switch.

The Altitude AP is physically connected to a LAN infrastructure and establishes an IP connection to a Summit WM-Series Switch. The Altitude AP has no user interface. The only way to manage a Altitude AP is through the Summit WM-Series Switch.

All communication with the Summit WM-Series Switch is carried out using a UDP-based protocol to encapsulate IP traffic from the Altitude APs and direct it to the Summit WM-Series Switch. The Summit WM-Series Switch decapsulates the packets and routes them to the appropriate destinations, while managing sessions and applying policy.

Figure 6: The Altitude AP



The Altitude AP has two radios:

- a 5 GHz radio that supports the 802.11a standard

  The *802.11a standard* is an extension to 802.11 that applies to wireless LANs and provides up to 54 Mbps in the 5-GHz band. 802.11a uses an orthogonal frequency division multiplexing encoding scheme rather than FHSS or DSSS.

NOTE

The Altitude 350-2 access point will automatically discontinue transmission in case of either absence of information to transmit (no frames transmitted through Ethernet) or operational failure.

- a 2.4 GHz radio that supports both the 802.11g and 802.11b standards

  The *802.11g standard* applies to wireless LANs and specifies a transmission rate of 54 Mbps. The *802.11b (High Rate)* standard is an extension to 802.11 that specifies a transmission rate of 11 Mbps. Because 802.11g uses the same communication frequency range as 802.11b (2.4 GHz), 802.11g devices can co-exist with 802.11b devices on the same network

Either radio on the Altitude AP can be enabled or disabled in the user interface. Both radios can be enabled and offer service simultaneously.

The Altitude AP supports the full range of 802.11a:

5.15 to 5.25 GHz	U-NII Low Band
5.25 to 5.35 GHz	U-NII Middle Band
5.725 to 5.825 GHz	U-NII High Band
New 5.470 GHz to 5.725 GHz Band (when approved by FCC)	

WARNING!

The Altitude 350-2 utilizing the internal or detachable antennas are intended only for indoor use. This specifically applies when the 5.15 to 5.25 GHz band is enabled.

The U-NII bands (Unlicensed National Information Infrastructure) are three frequency bands of 100 MHz each in the 5 GHz band designated for short-range, high-speed wireless networking communication.

Altitude APs are licensed to operate in North America, the European Union countries and European Union free trade countries. The Altitude AP will operate on the radio band allowed for each European Union country, after being configured on the Summit WM-Series Switch in the *Altitude AP Configuration: Properties* screen.

The Altitude AP has two models:

- internal antenna (Altitude 350-2 Integrated Antenna), internal dual (multimode) diversity antennas
- external antenna (Altitude 350-2 Detachable Antenna) (dual external antennas), RP-SMA connectors

For North America, the U-NII Low Band (5.15 to 5.25 GHz band) is disabled for the Altitude 350-2 Detachable Antenna to comply with FCC regulations.

Installing the Altitude APs

Install the Altitude APs as described in the *Altitude AP Installation Guide* packed with the units.

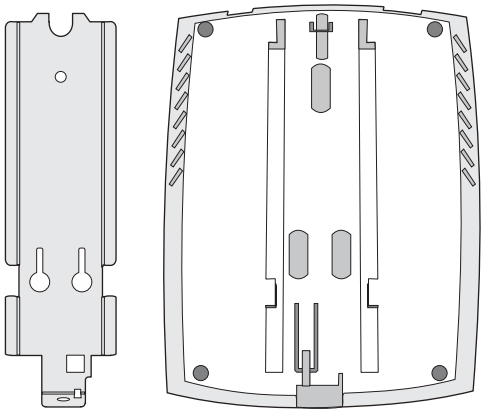
1 Unpack the Altitude AP from its shipment carton. Check that all parts are present, using the *Installation Guide* packed with the unit.

2 Mount the Altitude AP wall bracket, using 3 screws, near the LAN ethernet cable plug coming from the wall.

3 Press the back of the Altitude AP onto the bracket, aligning it with the open notches in the bracket. Then slide it downwards until it clicks into place.

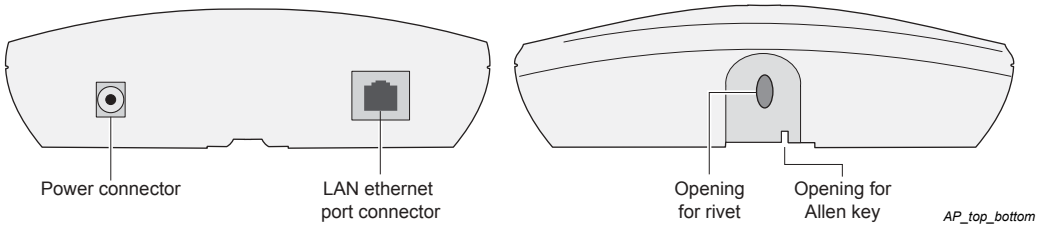
CAUTION

There should be at least 9 inches (20 cm) separation between the Altitude 350-2 and, or antenna and users.



To remove the Altitude AP, release the spring clip by inserting the Allen key (provided) into the small hole at the bottom of the bracket. Use the Allen key to depress the spring clip. Then slide the case up the bracket and lift off the Altitude AP. Keep the Allen key in a safe place.

4 Insert the plastic spreading rivet through the hole at the bottom of the bracket and into the Altitude AP case. Then screw in the plastic screw. This spreads the rivet and locks the case to the bracket. To remove the Altitude AP, use a screwdriver to take out the screw.



WARNING!

For installations that use Receive diversity (the default) the antennae should be pointed in the same direction. For installations that do NOT use Receive diversity or for those that split the 802.11a and 802.11b/g radio onto different physical ports, then the antennae can be pointed in whatever direction is desired.

Connecting and powering the Altitude AP

WARNING!

The Altitude 350-2 with internal and detachable antenna is intended for indoor use only. Device must not be connected to a LAN segment exposed to outdoor wiring. Ensure that all cables are installed to avoid strain. Replace the power supply adaptor immediately, if it shows any signs of damage.

Powering up the Altitude AP initiates its automatic discovery and registration process with the Summit WM-Series Switch, The parameters for this process should be set in the *Altitude AP Registration* screen.

WARNING!

Use only an UL approved Limited Power Source to provide power to the Altitude 350-2. This includes an UL/Safety approved Power over Ethernet (PoE) switch, UL/Safety approved power injector, or UL/safety approved (Class 2) AC wall adaptor.

Connect and power up the Altitude APs in one of three ways:

- Power Over Ethernet (PoE)

  If your network is already set up with PoE, attach the LAN ethernet cable to the RJ45 ethernet connector at the top of the Altitude AP.
- Power Over Ethernet: Adding PoE Injector

  If your network is not set up with PoE, you can provide power to the ethernet cable with a PoE injector. The PoE injector must be 802.3af compliant. The PoE injector is not provided with the Altitude AP.
- Power by AC Adaptor

  An AC adaptor is not provided with the Altitude AP. If you wish to use one, the specifications are: Input: 120-240 VAC, Output Voltage DC +6V, max amps 1.50, max watts 10.

To use an adaptor, install the Altitude AP within six feet of a wall outlet, attach the adaptor to the Altitude AP and then plug the adaptor into the wall outlet.

Discovery and registration: Altitude AP registration settings

Before the Altitude APs are powered and begin their "discovery" process, you should define the parameters of this process in the *Altitude AP Registration* screen. In this screen, you define two elements involved in the "discovery" process:

- Security Mode
- Discovery Timers

The **Stand-alone** or **Paired** options are part of the *Availability* feature to define a failover Summit WM-Series Switch if the primary Summit WM-Series Switch fails, described later in this Guide.

During the "Registration" process, the Summit WM-Series Switch's approval of the serial number of the Altitude AP depends on the security mode that has been set:

- Allow all
  If the Summit WM-Series Switch does not recognize the serial number, it sends a default configuration to the Altitude AP.
  If it recognizes the serial number, it sends the specific configuration (port and binding key) set for that Altitude AP.
- Allow approved
  If the Summit WM-Series Switch does not recognize the serial number, the operator is prompted to create a configuration.
  If it recognizes the serial number, it sends the configuration for that Altitude AP.

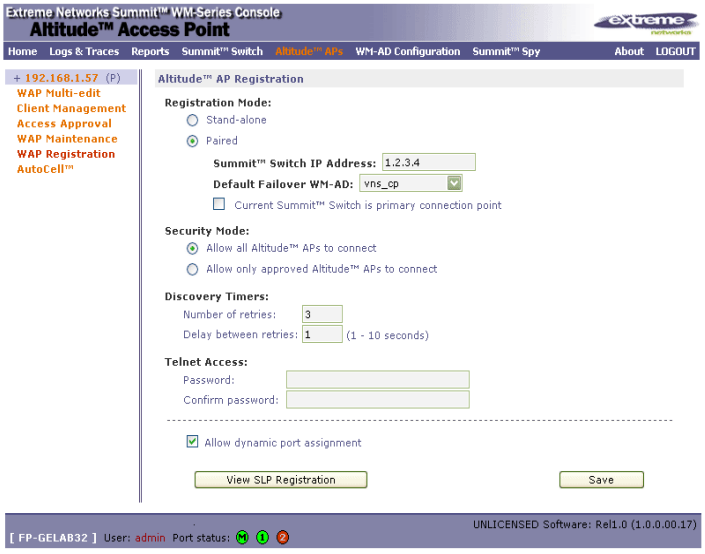
NOTE

It may be advisable, for the initial set up of the network, to select the "Allow All" option here. This is the most efficient way to get a large number of Altitude APs registered with the Summit WM-Series Switch.

After that, you may want to reset this option to "Allow Approved", so that no unapproved Altitude APs would be able to connect. You can modify the status of an unapproved Altitude AP in the Access Approval screen.

Define the Security Mode for registering Altitude APs

1 Select the **Altitude APs** tab in any screen. Click on **AP Registration**. The Altitude AP *Registration Mode* screen appears.



2 To **allow all** Altitude APs to connect, click this radio button (default mode)

To **allow only approved** Altitude APs to connect, click on this radio button.

Set the discovery timers

3 Define the timing parameters for the "discovery" process:

Number of Retries The default number of retries is 3.

Delay between Retries	The default is 1 second

4 To save the above parameters, click the **Save** button.

This completes the preparation for the “discovery” process. Now you can go back to the Altitude APs and power them on.

Discovery and registration

When the Altitude AP is powered on, it automatically begins a “discovery” process to determine the IP address of the Summit WM-Series Switch. When successful, it registers with the Summit WM-Series Switch.

When the Altitude AP is registered, it appears in the *Altitude AP Access Approval* screen. You can check its status in this screen. If the status is “Pending”, you must modify it to “Approved”.

You can now assign the registered and approved Altitude AP to a WM Access Domain Service (WM-AD) and it will be ready to handle wireless traffic.

Discovery steps

The Altitude APs “discover” the IP address of a Summit WM-Series Switch using a sequence of mechanisms that allow for the possible services available on the enterprise network.

The “discovery” steps are processed in the following order, until the Altitude AP successfully locates a Summit WM-Series Switch with which it can “register”.

1 Use the IP address of the last successful connection to a Summit WM-Series Switch.
2 Use the predefined static IP addresses for the Summit WM-Series Switchs on the network (if so configured).
3 Use Dynamic Host Configuration Protocol (DHCP) Option 78 to locate a Service Location Protocol (SLP) Directory Agent (DA), followed by a unicast SLP request to the Directory Agent.
4 Use a Domain Name Server (DNS) lookup for the host name “ext-summitwm-connect-1”.
5 Use a multicast SLP request to find SLP Service Agents (SAs).

You must ensure that the appropriate services on your enterprise network are prepared to support the “discovery” process.

Discovery step 1: last successful connection

Once a Altitude AP has successfully registered with a Summit WM-Series Switch, it remembers that controller's IP address, and will use that address on subsequent reboots. In effect, it will bypass discovery, and go straight on to registration. However, if this discovery method fails, it cycles through the remaining steps until it meets with success.

Discover step 2: static IP address

You can specify a list of static IP addresses of the Summit WM-Series Switches on your network. On the *Altitude AP Configuration* screen **Static Configuration** tab, add the addresses to the Summit WM-Series Switch Search List.

WARNING!

Care must be taken when setting or changing these values. Altitude APs configured statically will connect only to Summit WM-Series Switches in the list. Improperly configured Altitude APs will not be able to connect to a non-existent Summit WM-Series Switch address and therefore will not be able to receive a corrected configuration.

Discovery step 3: the DHCP and unicast SLP solution

To use the DHCP and unicast SLP discovery method, you must ensure that the DHCP server on your network supports Option 78 (DHCP for SLP RFC2610). The Altitude APs use this to discover the Summit WM-Series Switch.

This solution takes advantage of two services that are present on most networks:

- DHCP (Dynamic Host Configuration Protocol), the standard means of providing IP addresses dynamically to devices on a network.
- SLP (Service Location Protocol), a means of allowing client applications to discover network services without knowing their location beforehand. Devices advertise their services, using a Service Agent. In larger installations, a Directory Agent collects information from Service Agents and creates a central repository (SLP RFC2608).

The Summit WM-Series Switch contains an SLP Service Agent that, when it starts up, queries the DHCP server for Option 78 and if found, registers itself with the *Directory Agent* as service type “extreme”. The Summit WM-Series Switch contains a Directory Agent (slpd).

The Altitude AP queries DHCP servers for Option 78 in order to locate any Directory Agents. The Altitude AP's SLP *User Agent* will then query the DAs for a list of “extreme” Service Agents.

Option 78 needs to be set for the subnets connected to the ports of the Summit WM-Series Switch and the subnets connected to the Altitude APs. These should contain an identical list of Directory Agent IP addresses.

Discovery step 4: the DNS solution

If no Directory Agent is found, or if it has no “extreme” Service Agents registered, the Altitude AP will attempt to locate a Summit WM-Series Switch via DNS.

If you choose to use this method for discovery, place an “A” record in the DNS server for “ext-summitwm-connect-1”. The <domain-name> is optional, but if you use one, ensure that it is listed with the DHCP server.

Discovery step 5: the multicast SLP solution

If all of the preceding methods fail to locate a Summit WM-Series Switch, then the Altitude AP sends out a multicast SLP request, looking for any SLP Service Agents providing the “extreme” service.

Registration after discovery

Any of the discovery steps 2 through 5 can inform the Altitude AP of a list of multiple IP addresses to which the Altitude AP may attempt to connect. Once the Altitude AP has "discovered" these addresses, it sends out connection requests to all of them simultaneously. It will attempt to register only with the first which responds to its request.

When the Altitude AP obtains the IP address of the Summit WM-Series Switch, it connects and registers, sending its serial number identifier to the Summit WM-Series Switch, and receiving from the Summit WM-Series Switch a port IP address and binding key.

Once a Altitude AP is registered with a Summit WM-Series Switch:

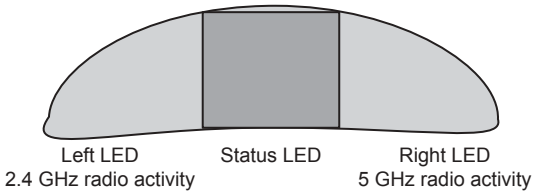
- it appears in the *Altitude AP Access Approval* screen. You can check its status in this screen. If the registration mode was "Approved only" then the status will be "Pending". You must modify it to "Approved".
- it appears in the side list in the *Altitude AP Configuration: Properties* screen, where you can modify the properties and radio parameters.
- its two radios appear as available choices in the *WM Access Domain Configuration: Topology* screen, when you are setting up a WM-AD (up to four WM-ADs for each radio).

Before a registered Altitude AP can handle wireless traffic, you must set up a WM-AD definition and assign the Altitude AP's radios to a WM-AD. See Chapter 6.

Discovery and registration: Altitude AP LED sequence

As the Altitude AP is powered on and boots up, you can follow its progress through the registration process by observing the LED sequence described below.

The Status LED (center) also indicates power: dark when unit is off and green (solid) when the AP has completed discovery and is operational.



The Altitude AP boot sequence is described below:

1 When powered on, the Altitude AP status LED turns from dark to green briefly.

Status LED: green (solid) then to dark before beginning boot sequence.

2 The Altitude AP performs a self-test.

Status LED: red (solid) if POST failed.

3 The "Discovery" mode: the Altitude AP sends a request to the DHCP server on the enterprise network for the location of the Summit WM-Series Switch (as described above.)

Status LED: orange (solid) while searching ("Discovery")

Status LED: red-orange (alternate blink) if DHCP server not found on network

Status LED: green-orange (alternate blink) if SLP issues in failed discovery.

4 The Altitude AP "learns" the IP address of the Summit WM-Series Switch,

Status LED: orange (blink) when IP address successfully obtained ("Registration" process underway)

Status LED: red (blink) if "Registration" fails

5 The Altitude AP sends its serial number (a unique identifier that is hard coded during manufacture) to the Summit WM-Series Switch.

Status LED: green (blink) when Altitude AP finds Summit WM-Series Switch ("Standby" status)

6 The Summit WM-Series Switch sends the Altitude AP a port IP address and a binding key, as follows:

- If the Summit WM-Series Switch does not recognize the serial number, it sends a default configuration to the Altitude AP.
- If it does recognize the serial number, it sends the specific configuration (port and binding key) set for that Altitude AP.

The Summit WM-Series Switch also adds the Altitude AP to its database.

Status LED: green (blink) when Altitude AP finds Summit WM-Series Switch ("Standby" status)

7 When the binding key is received, the Altitude AP's status changes from "Standby" to "Active". It becomes active and is enabled to transmit data traffic.

LED: green steady ("Active")

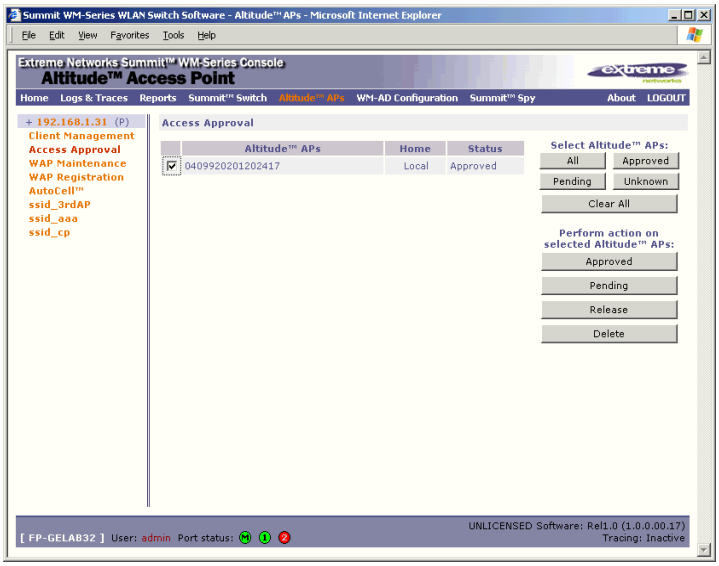
When the Altitude AP has wireless traffic, you will see a green blink on the traffic LED. The left LED indicates the traffic LED for activity on the 2.4 GHz radio, while the right LED indicates activity on the 5 GHz radio.

Altitude AP access approval

You can also view and modify the status of registered Altitude APs. Use this function to modify the status of a Altitude AP from "Pending" to "Approved" for a manual registration. You can also delete the configuration of Altitude APs that are no longer in service.

Modify a Altitude AP's registration status (approve access)

1 Click on the **Altitude APs** tab. The *Altitude AP Configuration* screen appears. Click on the **Access Approval** option. The *Access Approval* screen appears, displaying the current registered Altitude APs and their current status.



The **Home** field displays “Local” (this Summit WM-Series Switch) or “Foreign” (other Summit WM-Series Switches), if you have set up two Summit WM-Series Switches in Paired Mode, as described in the *Summit WM-Series Switch Configuration: Availability* topic.

2 Select the Altitude APs for status change, either by:

- clicking the checkbox on to select a specific Altitude AP, or
- using one of the **Select Altitude APs** buttons to select by category

3 To perform an action on the selected Altitude APs, click on one of the **Action** buttons: Approved, Pending, Release, Delete.

- Change a Altitude AP's status from “Pending” to “Approved”, if the Altitude AP *Configuration: AP Registration* screen was set to register only approved Altitude APs.
- Release “foreign” Altitude APs after recovery from a Failover, as described in the *Availability* topic.

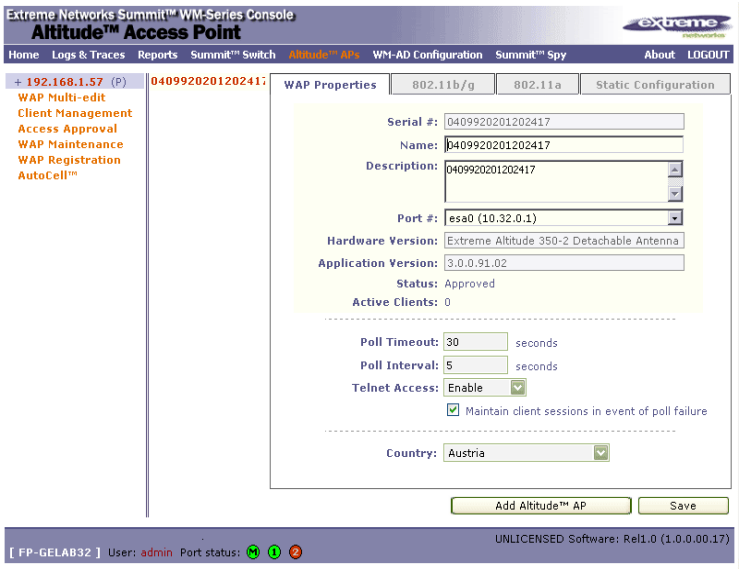
Configuring properties and radios

Once a Altitude AP has successfully registered on the Summit WM-Series Switch, it appears in the side list in the Altitude AP *Configuration: Properties* screen, where you can modify its properties and radio parameters.

View and modify properties of registered Altitude APs

1 Select the **Altitude APs** tab in any screen. The Altitude AP *Configuration* screen appears, with a list of registered Altitude APs.

2 Highlight the appropriate Altitude AP in the list. Click on the **AP Properties** tab to view basic information about the highlighted Altitude AP.



3 To modify the default information about a selected Altitude AP, key in information in the following fields (where appropriate):

Serial #	(Display only) A unique identifier set during manufacture.
Name	Defaults to the serial number. Change this to a unique descriptive name that more easily identifies the Altitude AP.
Description	Available for descriptive comments (optional).
Port #	From the drop-down list, select the ethernet port through which the Altitude AP can be reached.
Hardware Version	(Display only) Current version of the Altitude AP hardware.
Application Version	(Display only) Current version of the Altitude AP software.
Status	(Display only) "Approved" = Altitude AP has received its binding key from the Summit WM-Series Switch after the Discovery process. "Pending" = binding key not yet received. You can modify the status of a Altitude AP (for example from "Pending" to "Approved") in the *Access Approval* screen.
Active Clients	(Display only) The number of wireless devices currently active on the Altitude AP.
Poll Timeout	The default is 30 seconds.
Poll Interval	The default is 5 seconds.

4 If this Altitude AP is to used in Bridge Mode as part of a static configuration for Branch Office deployment, click the **Maintain client session in event of poll failure** checkbox on in order to maintain the session. See "Altitude AP static configuration: branch office deployment" on page 57.

5 To save the modified information, click on the Save button.

View and modify the radio settings of registered Altitude APs

Most properties of the Altitude AP radios can be modified without triggering a reboot of the Altitude AP. However, modifying the following will trigger a reboot:

- enabling or disabling either radio
- changing the radio channel between "Auto" and any fixed channel number.

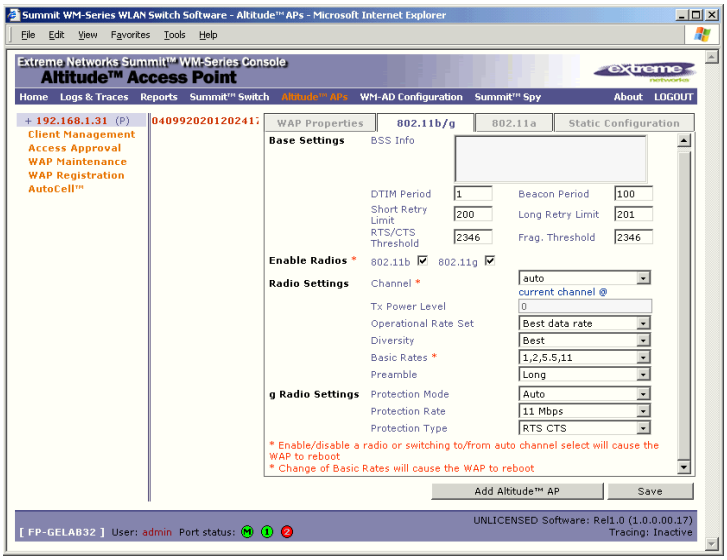
View and modify the radio settings

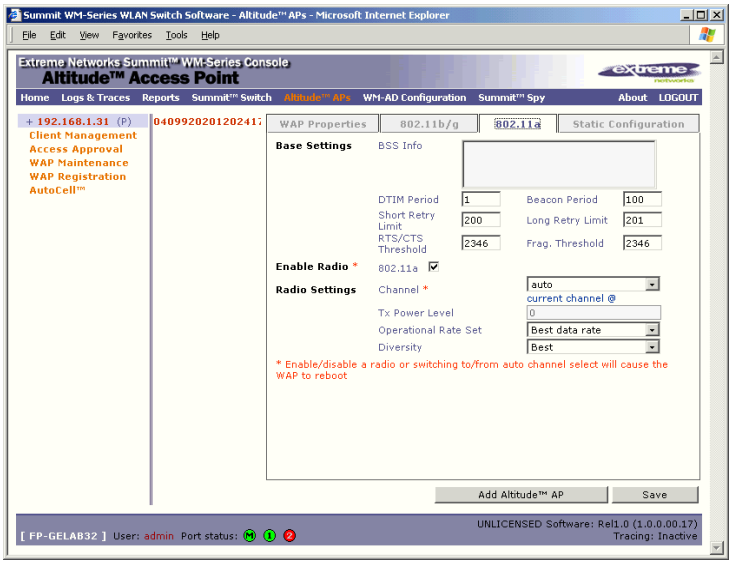
1 Select the **Altitude APs** tab in any screen. The *Altitude AP Configuration* screen appears, with a list of registered Altitude APs.

2 Highlight the appropriate Altitude AP in the list. Then click on either radio tab:

- 802.11 b/g (2.4 GHz radio)
- 802.11a (5 GHz radio)

Each screen displays the default radio settings for each radio on the Altitude AP. If this radio has been assigned to a WM-AD (up to four WM-ADs), the WM-AD names and MAC addresses appear in the Base Settings area.





3 Modify these **Base Settings** where appropriate.

BSS Info	(Display only) After WM-AD configuration, the Basic Service Set (BSS) area displays the MAC address on the Altitude AP for each WM-AD and the SSIDs of the WM-AD to which this radio has been assigned.
DTIM	Delivery Traffic Indication Message period. Default is 2.
Beacon Period	Time units between beacon transmissions. Default is 100.
Short Retry Limit	The maximum number of transmission attempts of a frame that is less than or equal to the RTS Threshold, before a failure condition is indicated. Default is 4.
Long Retry Limit	The maximum number of transmission attempts of a frame that is greater than the RTS Threshold, before a failure condition is indicated. Default is 7.
RTS Threshold	Request To Send Threshold, the size of a data unit below which an RTS/CTS (RTS/Clear to Send) handshake is not performed. Default is 2330.
Frag. Threshold	The Fragmentation Threshold, the maximum size of a packet or data unit that can be delivered. Default is 2346.
Enable Radios	Click checkbox on for each radio.
Radio Settings:	
Channel	(Drop-down list) The wireless channel that the Altitude AP should use to communicate with wireless devices (*see chart below*). Depending on the regulatory domain (based on country), some channels may be restricted. The default setting is based on North America.
Tx Power Level	(Drop-down list) Min, 13%, 25%, 50%, Max If Auto Cell was enabled in the previous window, it will override selections made here in the **Tx Power Level** field.
Operational Rate Set	(Drop-down list) in Mbps A: Best data rate, 6, 9 12,18, 24, 36, 48, 54 B/G: Best data rate, 1, 2, 5.5, 11, 6, 9 12,18, 24, 36, 48, 54
Diversity	From the drop-down list, select “Best,” for the best signal from both antennas, or “Left” or “Right” to choose either of the two diversity antennas.
Basic Rates	(for b radio only) Select a set of basic rates from the drop-down list. The best data rate from the set will be used for current conditions (power vs. range)
Short Preamble Invoked	Click checkbox on to enable.
g Radio Settings:	
Protection Mode	(Drop-down list) None, Auto (default), Always
Protection Rate	(Drop-down list) in Mbps: 1, 2, 5.5, 11 (default)
Protection Type	(Drop-down list) CTS (Clear To Send), RTS CTS (Request To Send, Clear To Send) - default.

NOTE

Radio A Channels 100 to 140 occupy the 5470-5725 MHz band, in the regulatory domains of the European Union and European Union free trade countries.

Radio B/G Channels 12 to 14 are not available in North America.

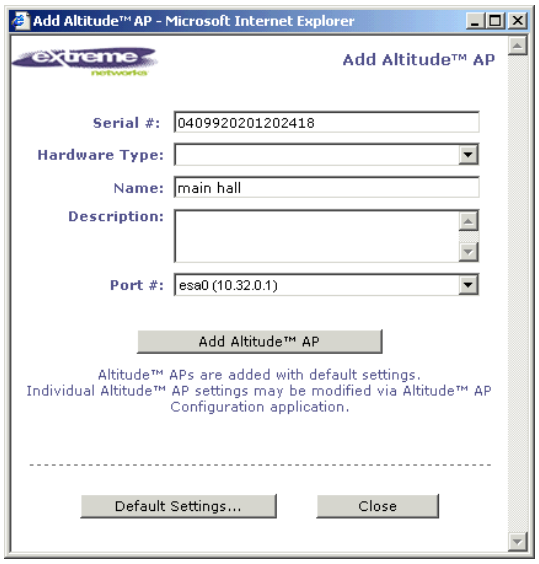
Radio Channels 802.11a	**Radio Channels 802.11b/g**
Auto	1: 2412 MHz
34: 5170 MHz	2: 2417 MHz
36: 5180 MHz	3: 2422 MHz
38: 5190 MHz	4: 2437 MHz
40: 5200 MHz	5: 2432 MHz
42: 5210 MHz	6: 2437 MHz
44: 5220 MHz	7: 2442 MHz
46: 5230 MHz	8: 2447 MHz
48: 5240 MHz	9: 2452 MHz
52: 5260 MHz	10: 2457 MHz
56: 5280 MHz	11: 2462 MHz
60: 5300 MHz	12 2467 MHz
64: 5320 MHz	13: 2472 MHz
100:	14: 2484 MHz
104:	
108:	
112:	
116:	
120:	
124:	
128:	
132:	
136:	
140:	
149: 5745 MHz	
153: 5765 MHz	
157: 5785 MHz	
161: 5805 MHz	

4 To save the modified information, click on the **Save** button.

Adding a Altitude AP manually

Add and register a Altitude AP manually:

1 Select the Altitude AP tab. In any radio screen, click on the **Add Altitude AP** button. The *Add Altitude AP* subscreen appears.



2 Key in, or select from the drop-down list, information in the following fields:

Serial #	A unique identifier set during manufacture.
Name	A unique name for the Altitude AP.
Description	Available for descriptive comments (optional).
Port #	The ethernet port through which the Altitude AP can be reached

3 To add the Altitude AP, click the **Add Altitude AP** button.

To return to the previous screen, click **Close**.

The Altitude AP is added with default settings. To modify these settings, use the Altitude AP Configuration screens described earlier. You can modify the properties and the settings for each radio on the Altitude AP.

Before a registered Altitude AP can handle wireless traffic, you must set up a WM-AD definition, and assign one or both of the Altitude AP's radios to a WM-AD. See Chapter 6 for details.

Altitude AP static configuration: branch office deployment

The Altitude AP static configuration feature provides Summit WM-Series Switch Software capability for a network with the central office / branch office model. In this scenario, Altitude APs are installed in remote sites, while the Summit WM-Series Switch is in the central office. The Altitude APs require the capability to interact in both the local site network and the central network. To achieve this, a static configuration is used.

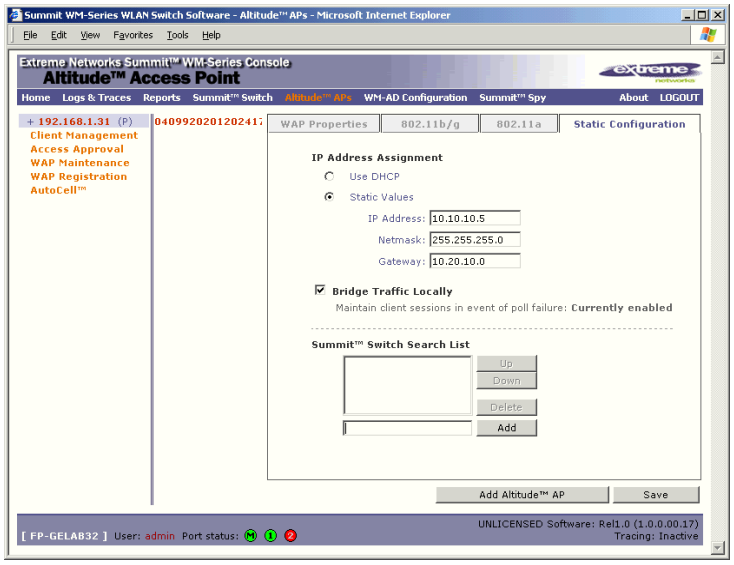
NOTE

In static configuration, if the Altitude AP cannot register with the Summit WM-Series Switch within the specified number of retries), the Altitude AP will use SLP, DNS and SLP multicast as a backup mechanism (as described in the discovery process). If unsuccessful, the Altitude AP resumes the discovery process with the static configuration, followed with SLP, DNS and SLP multicast.

Once the static configuration is set up, then all traffic is bridged locally on the wired Ethernet segment that the Altitude AP is connected to, without going through a Summit WM-Series Switch.

Set up a Altitude AP with static configuration

1 Select the **Altitude AP** tab in any screen. In the Altitude AP **Properties** screen, click on the **Static Configuration** tab. The *Static Configuration* screen appears.



2 Select one of the two methods of IP address assignment for the Altitude AP:

- to enable **DHCP**, click the radio button on (default), or
- to specify the IP address of the Altitude AP, click the **Static Values** radio button on and fill in the IP Address, Subnet Mask, and Gateway.

NOTE

For first-time deployment of the Altitude AP for a Branch Office scenario, it is recommended that you use DHCP initially on the central office network to obtain an IP address for the Altitude AP. Then enter these values in the Static Configuration screen for this Altitude AP and save the configuration.

3 Click the **Bridge Traffic Locally** checkbox on to enable this. When authentication of a wireless device user in the Branch Office is complete, the Altitude AP will direct all traffic to the local network.

   Authentication is 802.1x-AAA. Authentication by Captive Portal is not supported

4 In the **Summit WM-Series Switch Search List** area of the screen, in the entry field, key in the IP address of the Summit WM-Series Switch that will control this Altitude AP. Click on the **Add** button to add it to the list. Repeat to add a secondary Summit WM-Series Switch. Use the **Up** and **Down** buttons to modify the order of the controllers (maximum 3 controllers).

   This allows the Altitude AP to bypass the discovery process. If this field is not filled in, the Altitude AP will use SLP to discover a Summit WM-Series Switch.

   The DHCP function for wireless clients must be provided locally by a local DHCP server, unless each wireless client has a static IP address

5 To save the static configuration, click on the **Save** button.

NOTE

In a "Branch Office" scenario, where the Altitude AP is configured statically on a local network whose MTU is lower than 1500, the Summit WM-Series Switch automatically adjusts the MTU size to prevent packet fragmentation. The MTU is set in the IP Addresses screen and should not be changed.

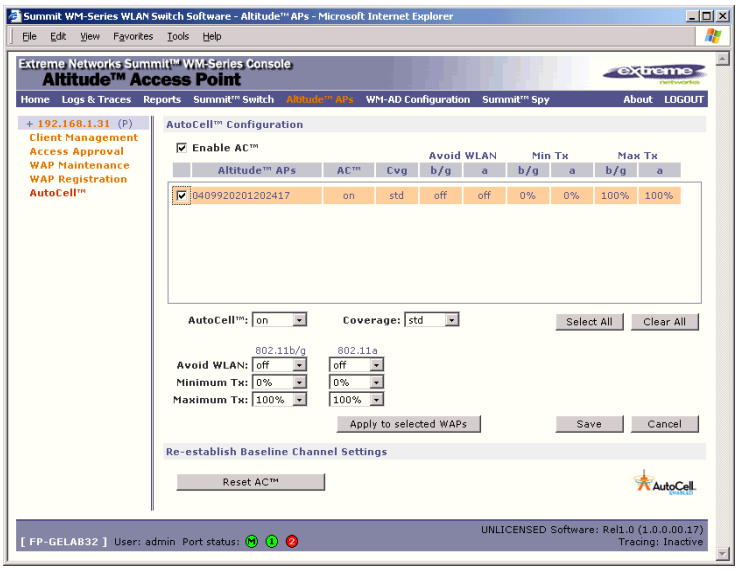
Auto Cell software

You can enable the Auto Cell software on the Altitude AP. With the Auto Cell feature enabled, the Altitude AP will:

- adjust power levels to balance coverage if another Altitude AP which is assigned to the same SSID and is on the same channel is added to, or leaves, the network.
- allow wireless clients to be moved to another Altitude AP if the load is too high
- scan automatically for a channel, using a channel selection algorithm
- avoid other WLANs by reducing transmit power whenever other APs with the same channel, but different SSIDs are detected

Configure Auto Cell software

1 Select the **Altitude AP** tab in any screen. Click on the **Auto Cell** option. The *Auto Cell Configuration* screen appears.



2 The **Enable Auto Cell** checkbox is on by default., enabling the software globally.

3 From the list of registered Altitude APs, select the Altitude AP you want to configure for Auto Cell by clicking its checkbox on.

The fields for Auto Cell populate with default values, with Auto Cell "on".

4 In the **Coverage** field, select from the drop-down list:

- **Std** (Standard Coverage) adjusts the range to the client that is the most distant, as indicated by its signal strength
- **Shpd** (Shaped Coverage) adjusts the range based on neighboring Altitude APs

5 To enable the **Avoid WLAN** feature, select **on** from the drop-down list.

6 To configure a range within which the transmit power can be adjusted dynamically, select the **Minimum** and **Maximum** power levels from the drop-down list.

7 When the configuration choices are complete, click on the **Apply to selected APs** button.

8 To save these changes, click on the **Save** button.

9 To re-establish baseline settings, forcing the APs to go through the auto-channel selection process, click on the **Reset Auto Cell** button.

5 WM Access Domain Services (WM-AD): Introduction

Overview

WM Access Domain Services (WM-AD) are the key to the advantages that the Summit WM-Series Switch Software system has to offer. This technique provides a versatile means of mapping wireless networks to the topology of an existing wired network.

When you set up a WM-AD on the Summit WM-Series Switch, you are defining a subnet for a group of wireless device users. This WM-AD definition creates a virtual IP subnet where the Summit WM-Series Switch acts as a default gateway to wireless devices.

Before you begin to define a WM-AD, you should have determined:

- a user access plan for both individual users and user groups
- the RADIUS attribute values that support the user access plan
- the location and identity of the Altitude APs that will be used on the WM-AD
- the routing mechanism to be used on the WM-AD
- the network addresses that the WM-AD will use
- the type of authentication for wireless device users on the WM-AD
- the specific filters to be applied to the defined users and user groups to control network access
- what privacy mechanisms should be employed between the Altitude APs and the wireless devices
- whether the WM-AD is to be used for voice traffic

The *user access plan* should analyze the enterprise network and identify which users should have access to which areas of the network. What areas of the network should be separated? Which users can go out the World Wide Web?

The Summit WM-Series Switch Software system relies on authenticating users via a RADIUS server (or other authentication server). To make use of this feature, you will, of course, require such an authentication server on the network. Make sure that the server's database of registered users, with login identification and passwords, is current.

NOTE

To deploy Summit WM-Series Switch Software without a RADIUS server (and without authentication of users on the network), select ***SSID*** *for network assignment (in the* Topology *screen). In the* Authentication - *Configure Captive Portal screen, click on the* ***No Captive Portal*** *radio button. There will be no authentication of users, but Summit WM-Series Switch Software is otherwise operational.*

The *user access plan* should also identify the user groups in your enterprise, and the business structure of the enterprise network., such as:

- department (such as Engineering, Sales, Finance)
- role (such as student, teacher, library user)
- status (such as guest, administration, technician)

For each user group, you should set up a Filter ID attribute in the RADIUS server, and then associate each user in the RADIUS server to at least one Filter ID name. The Summit WM-Series Switch Software enables you to define specific filtering rules, by Filter ID attribute, that will be applied to user groups to control network access.

What is a WM-AD?

A WM-AD is an IP subnet that is especially designed to enable Altitude APs to interact with wireless devices. In many ways, a WM-AD is similar to a regular IP subnet. However, it has the following required features:

1 Each WM-AD is assigned a unique identifier.

2 Each WM-AD is assigned an SSID. These do not have to be unique.

3 Each WM-AD is assigned a range of IP addresses for wireless devices. All the wireless devices share the same IP address prefix (the part of the IP address that identifies the network and subnet).

The IP addresses of the wireless devices are assigned dynamically by the Summit WM-Series Switch's DHCP server within the assigned range.

(These IP addresses are not “virtual”. They are regular IP addresses, and are unique over the network. These IP addresses are advertised to other hosts on the network so that they can exchange traffic with the wireless devices in the WM-AD.)

NOTE

Alternatively, you can allow the enterprise network's DHCP server to provide the IP addresses for the WM-AD, by enabling DHCP Relay in the Topology *screen.*

4 A single overall filtering policy applies to all the wireless devices within the WM-AD. Further filtering can be applied when the wireless user is authenticated by the RADIUS server.

5 When the Summit WM-Series Switch creates the WM-AD, it also creates a virtual IP subnet for that WM-AD.

6 Each WM-AD represents a mobility group that, when configured, can be carried across multiple Summit WM-Series Switches.

7 Each WM-AD also offers unique AAA services.

Topology of a WM-AD

Before you configure a WM-AD, you should define global settings that will apply to all WM-AD definitions. In the *Global Settings* screen, identify the location of the RADIUS servers. You also enable Priority Traffic Handling for voice-over-internet traffic.

In the *Topology* screen, you name a new WM-AD and begin its configuration

The key choice for a WM-AD is the type of network assignment, which determines all the other factors of the WM-AD. There are two options for network assignment:

- SSID:
  - has Captive Portal authentication, or no authentication.
  - requires restricted filtering rules before authentication and, after authentication, filtering rules for group Filter IDs.
  - is used for a WM-AD supporting wireless voice traffic (QoS).
  - is used for a WM-AD supporting third-party APs.
  - has WEP and WPA-PSK privacy.
- AAA (Authentication, Authorization and Accounting)
  - has 802.1x authentication
  - requires filtering rules for group Filter IDs and default filter.
  - has WEP and WPA privacy.

In the *Topology* screen, you assign the available Altitude APs (by radio) to the WM-AD. An Altitude AP radio will appear in the list as available for WM-AD assignment until it has been assigned to four WM-ADs. After that, it will no longer appear in the list.

After a WM-AD definition has been saved, the Summit WM-Series Switch updates this information on the Altitude AP. Each radio acquires up to four SSIDs (one for each WM-AD it is part of), and broadcasts these during beacon transmission (unless the SSID beacon is suppressed in the *Topology* screen).

You can view (in the *Altitude AP Configuration* screen) a list of defined WM-ADs to which each radio has been assigned.

In the *Topology* area of WM Access Domain Configuration, you also define other aspects of the WM-AD, such as the parameters for DHCP for IP address assignment. You might also configure this WM-AD for management traffic only, or for Third-Party Access Points, or for Voice Traffic. (These are described in detail later in this Guide.)

Network assignment and authentication for a WM-AD

The second step is to configure the authentication mechanism for the WM-AD. The authentication mechanism depends on the network assignment. In addition, all WM-AD definitions can include authentication by MAC address.

Authentication with SSID network assignment

If **SSID** was selected, there are two authentication options:

- None: The wireless device connects to the network, but can only access specified network destinations (defined in the Non-Authenticated Filter). No authentication is performed.
- Captive Portal: The wireless device connects to the network, but can only access specified network destinations (defined in the Non-Authenticated Filter). One of those destinations is a web page logon screen (the portal in which he is captive), where the user must input an ID and a password. This

identification is sent by the Summit WM-Series Switch to the RADIUS server for authentication. Four authentication types are supported by Summit WM-Series Switch Software for Captive Portal:

- PAP (Password Authentication Protocol)
- CHAP (Challenge Handshake Authentication Protocol)
- MS CHAP (Windows-specific version of CHAP)
- MS CHAP v2 (Windows-specific version of CHAP, version 2)

For Captive Portal, the RADIUS server must support the selected authentication type: PAP, CHAP (RFC2484), MS-CHAP (RFC2433), MS-CHAPv2 (RFC2759).

Authentication with AAA (802.1x) network assignment

If network assignment is by **AAA (802.1x)** with 802.1x authentication, the wireless device user requesting network access via Summit WM-Series Switch Software must first be authenticated. The wireless device's client utility must support 802.1x. The user's request for network access along with login identification or user profile will be forwarded by the Summit WM-Series Switch to a RADIUS server. Summit WM-Series Switch Software supports these authentication types:

- EAP-TLS Extensible Authentication Protocol - Transport Layer Security that relies on client-side and server-side certificates to perform authentication and can be used to dynamically generate user-based and session-based WEP keys.
- EAP-TTLS (EAP with Tunneled Transport Layer Security) is an extension of EAP-TLS to provide certificate-based, mutual authentication of the client and network through an encrypted tunnel, as well as to generate dynamic, per-user, per-session WEP keys. Unlike EAP-TLS, EAP-TTLS requires only server-side certificates.
- PEAP (Protected Extensible Authentication Protocol) is a standard to authenticate wireless LAN clients without requiring them to have certificates. In PEAP authentication, first the user authenticates the authentication server, then the authentication server authenticates the user.

For 802.1x, the RADIUS server must support RADIUS extensions (RFC2869).

If the RADIUS server sends an “access-accept” message to the Summit WM-Series Switch, the Summit WM-Series Switch's DHCP server assigns the device its IP address and allows network access controlled by the filtering rules defined for the specific Filter ID value associated with the wireless device user.

Both Captive Portal and AAA (802.1x) authentication mechanisms in Summit WM-Series Switch Software rely on a RADIUS server on the enterprise network. You can identify and prioritize up to three RADIUS servers on the Summit WM-Series Switch. This means that in the event of a failover of the active RADIUS server, the Summit WM-Series Switch will poll the other servers in the list for a response.

Filtering for a WM-AD

The WM-AD capability provides a technique to apply policy, to allow different network access to different groups of users. This is done by packet filtering.

After setting up the authentication, the next step is to define the filtering rules for the filters that apply to your network and the WM-AD you are setting up.

Four types of filters are applied by the Summit WM-Series Switch in the following order:

1. Exception filter, to provide the administrator optional additional flexibility in securing the system and blocking Denial of Service (DoS) attacks, on any type of WM-AD.
2. Non-Authenticated filter, with filtering rules that apply before authentication, to control network access and to direct users to a Captive Portal web page for login.
3. Group filters (by Filter ID) for designated user groups, to control access to certain areas of the network, with values that match the values defined for the RADIUS Filter ID attribute.
4. Default filter, to control access if there is no matching Filter ID for a user.

Within each type of filter, you define a sequence of filtering rules. This sequence must be carefully planned and arranged in the order that you want them to take effect. You define each rule to either allow or deny traffic in either direction:

- "In": from a wireless device in to the network
- "Out": from the network out to the wireless device

The final rule in any filter should be a catch-all for any traffic that did not match a filter. This final rule should either "allow all" or "deny all" traffic, depending on the requirements for network access. For example, the final rule in a *Non-Authenticated Filter* for Captive Portal is typically "deny all". A final "allow all" rule in a Default Filter will ensure that a packet is not dropped entirely if no other match can be found.

Each rule can be based on any *one* of the following:

- destination IP address, or any IP address within a specified range that is on the network subnet (as a wildcard)
- destination ports, by number and range
- protocols (UDP, TCP, etc.)

This is how the Summit WM-Series Switch software filters traffic:

1. The Summit WM-Series Switch software attempts to match each packet of a WM-AD to the filtering rules that apply to the wireless device user.
2. If a filtering rule is matched, the operation (allow or deny) is executed.
3. The next packet is fetched for filtering.

The filtering sequence depends on the type of authentication:

- No authentication (network assignment by SSID)

  Only the Non-Authenticated filter will apply. Specific network access can be defined. Since there will be no authentication, the final rule should be "deny all".
- Authentication by captive portal (network assignment by SSID)

  The Non-Authenticated filter will apply before authentication. Specific network access can be defined. The filter should also include a rule to allow all users to get as far as the Captive Portal webpage where the user can enter login identification for authentication. When authentication is returned, then the Filter ID group filters are applied. If no Filter ID matches are found, then the Default filter is applied.

- Authentication by AAA (802.1x)

  Since users have already logged in and have been authenticated, there is no need for a Non-Authenticated filter. When authentication is returned, then the Filter ID group filters are applied. For AAA, a WM-AD can have a subgoup with Login-LAT-group ID that has its own filtering rules. If no Filter ID matches are found, then the Default filter is applied.

Privacy on a WM-AD: WEP and WPA

Privacy is a mechanism that protects data over wireless and wired networks, usually by encryption techniques. Summit WM-Series Switch Software supports:

- Wired Equivalent Privacy (WEP) which encrypts data sent between wireless nodes. Each node must use the same encryption key.
- Wi-Fi Protected Access (WPA v.1 and WPA v.2) privacy, in Enterprise Mode (which specifies 802.1x authentication and requires an authentication server) or in Pre-Shared Key (PSK) mode (which relies on a shared secret). Encryption is by Advanced Encryption Standard (AES) or by Temporal Key Integrity Protocol (TKIP). If WPA v.2 is selected, both WPA v.1 and WPA v.2 are supported simultaneously, defaulting to the highest encryption method.

Setting up a new WM-AD

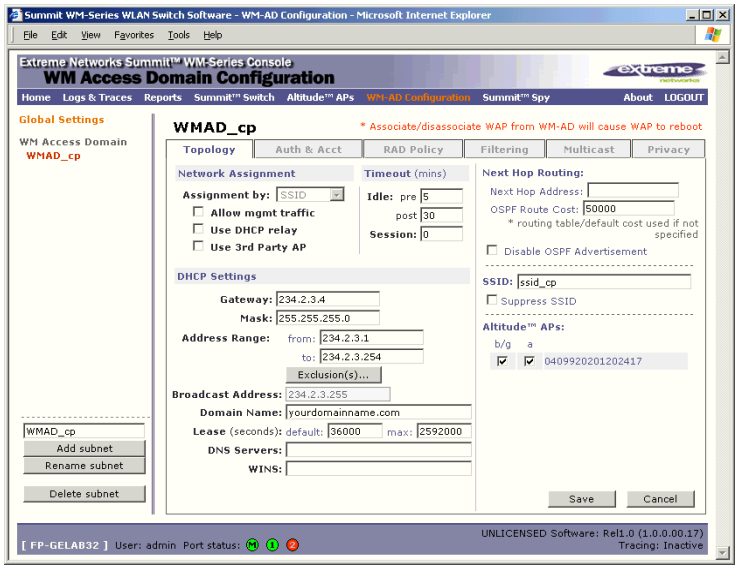
Click on the **WM-AD Configuration** tab in any screen. The *WM Access Domain Configuration* screen appears. For a new Summit WM-Series Switch Software installation, where no WM-AD has yet been defined, the screen is blank, except for the **Add subnet** function.

Create a new WM-AD name

1 In the entry field above the **Add subnet** button, key in a name that will uniquely identify the new WM-AD.

2 Click on the **Add subnet** button. The name appears in the left-hand list. The *Topology* screen appears.

3 In the left-hand list, highlight the name of the new WM-AD. You can now configure its parameters in the *Topology* screen.



Configure the new WM-AD (overview of basic steps)

1 Select the network assignment mechanism from the **Assignment by** drop-down list:

- SSID
- AAA

2 In the SSID box at the right, key in the SSID that the wireless devices will use to access the Altitude AP.

3 Select the **Altitude APs** (by radio) to be assigned to this WM-AD. The displayed list of available **Altitude APs** has a checkbox for each radio on the Altitude AP. Each radio on a Altitude AP can be assigned to a maximum of four WM-ADs. When this maximum is reached, the radio will no longer be available in this list.

4 Configure other options for this WM-AD: Allow Management Traffic, Use DHCP Relay, Use 3rd Party APs, or Enable Priority Traffic Handling.

5 Define the DHCP settings for this WM-AD.

6 To save the new WM-AD Topology, click on the **Save** button.

When the new Topology has been saved, the screen displays tabs for *Auth & Acct*, *RAD Policy*, *Filtering*, *Multicast*, and *Privacy*, for configuring these aspects of the new WM-AD.

Before you configure the WM-AD, you must first define the Global Settings.

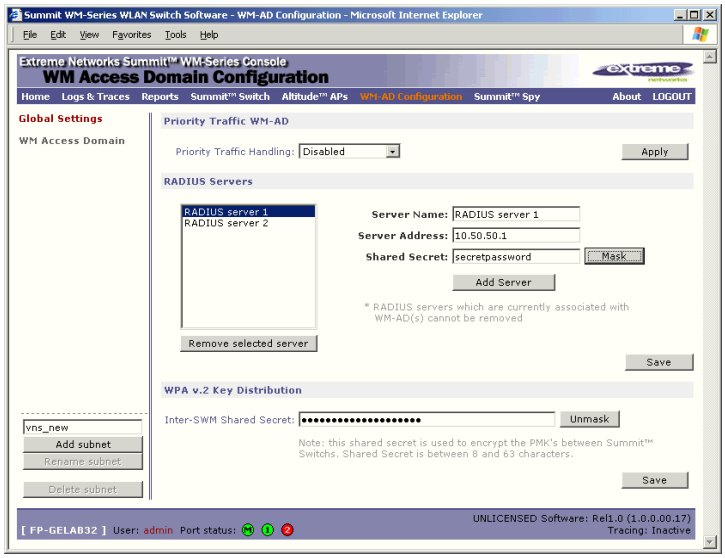
Global Settings for a WM-AD

Before defining specific WM Access Domain Service (WM-AD), define various settings that will apply to all WM-AD definitions. These global settings include:

- enabling or disabling Priority Traffic Handling for voice-over internet traffic
- identifying the location and password of RADIUS servers on the enterprise network

  The servers defined here will appear as available choices when you set up the authentication mechanism for each WM-AD.
- defining the shared secret used to encrypt the Pairwise Master Key (PMK) for WPA v.2 between Summit WM-Series Switchs on the network

1 In the *WM Access Domain Configuration* screen, in the left-hand list click on the **Global Settings** option.


Summit WM-Series WLAN Switch Software - WM-AD Configuration - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Extreme Networks Summit™ WM-Series Console
WM Access Domain Configuration
Home Logs & Traces Reports Summit™ Switch Altitude™ APs WM-AD Configuration Summit™ Spy About LOGOUT
Global Settings
WM Access Domain
Priority Traffic WM-AD
Priority Traffic Handling: Disabled
Apply
RADIUS Servers
RADIUS server 1
RADIUS server 2
Server Name: RADIUS server 1
Server Address: 10.50.50.1
Shared Secret: secretpassword
Mask
Add Server
* RADIUS servers which are currently associated with WM-AD(s) cannot be removed
Remove selected server
Save
WPA v.2 Key Distribution
Inter-SWM Shared Secret:
Unmask
Note: this shared secret is used to encrypt the PMK's between Summit™ Switchs. Shared Secret is between 8 and 63 characters.
Save
vns_new
Add subnet
Rename subnet
Delete subnet
[FP-GELAB32] User: admin Port status:
UNLICENSED Software: Rel1.0 (1.0.0.00.17)
Tracing: Inactive

Enable Priority Traffic Handling for a VoIP WM-AD

2 The **Priority Traffic Handling** field is disabled by default. After you have defined a WM-AD, its name will appear in the drop-down list. To prioritize voice-over-internet traffic on a WM-AD, select its name from the drop-down list.

3 To activate this setting, click on the **Apply** button.

Define the RADIUS servers available on the network

4 For each RADIUS server, fill in the following fields:

Server Name	Name of the RADIUS server
Server Address	The IP address of the RADIUS server
Shared Secret	The password that is required in both directions that is set up on the RADIUS Server. This password is used to validate the connection between the Summit WM-Series Switch and the RADIUS Server.

To display the shared secret (in order to proofread your entry before saving the configuration), click on the **Unmask** button. To mask the shared secret, click on the button again (the button toggles between **Mask** and **Unmask**). This precautionary step is recommended in order to avoid an error later when the Summit WM-Series Switch attempts to communicate with the RADIUS server.

5 To add the defined server to the list, click on the **Add** button.

6 To remove a defined server from the list, highlight it and click on the **Remove selected server** button.

7 To save these settings, click on the **Save** button.

Key distribution between Summit WM-Series Switches

8 Key in a shared secret (between 8 and 63 characters long) to be used between Summit WM-Series Switches. Mask or unmask as you type, as described above. The same shared secret must also be defined on the other Summit WM-Series Switches on the network.

9 To save this Shared Secret, click on the **Save** button.

6 WM Access Domain Configuration

For each WM-AD, you define its topology, authentication, accounting, RADIUS servers, filtering, multicast parameters and privacy mechanism. When you set up a new WM-AD definition, the additional tabs will appear only after you save the Topology.

Topology for a WM-AD

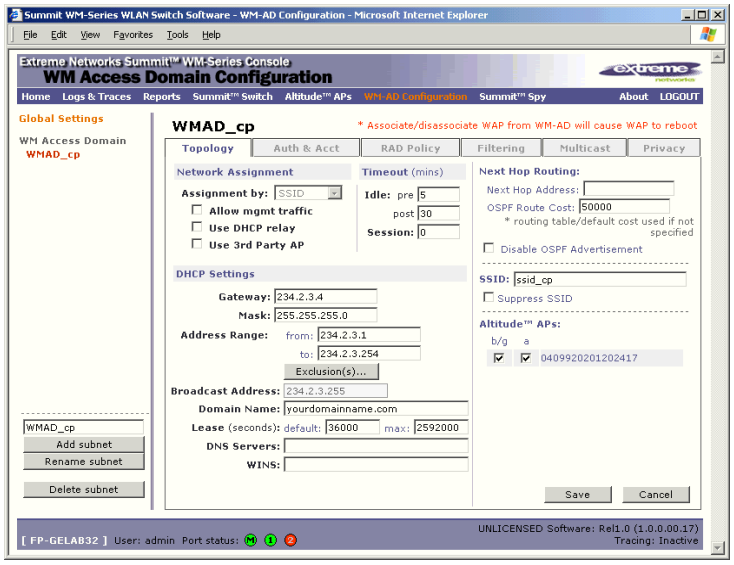
In the *Topology* screen, the key choice for a WM-AD is the type of network assignment, which determines all the other factors of the WM-AD. There are two options for network assignment:

- **SSID**:
  - has Captive Portal authentication, or no authentication (as well as MAC-based authentication).
  - requires restricted filtering rules before authentication and, after authentication, filtering rules for group Filter IDs.
  - is used for a WM-AD supporting wireless voice traffic (QoS).
  - is used for a WM-AD supporting third-party APs.
  - has WEP and WPA-PSK privacy.
- **AAA** (Authentication, Authorization and Accounting):
  - has 802.1x authentication (as well as MAC-based authentication)
  - requires filtering rules for group Filter IDs and default filter.
  - has WEP and WPA (WPA v.1 and WPA v.2) privacy.

Topology for a WM-AD for Captive Portal

The section describes how to set up a WM-AD for Captive Portal.

In the *WM Access Domain Configuration* screen, highlight the WM-AD name in the left-hand list and click on the **Topology** tab.



Create an SSID for Captive Portal WM-AD

1 Using the **Assignment by** drop-down list, select **SSID**.

2 In the **SSID** box, key in the SSID that wireless devices will use to access the Altitude AP.

3 Click the **Suppress SSID** checkbox on to prevent this SSID from appearing in the beacon message sent by the Altitude AP. The wireless device user seeking network access will not see this SSID as an available choice, and will need to specify it.

Define the Session Timeout parameters for this WM-AD

4 In the **Timeout** area, in the **Idle** "pre" field, key in the number of minutes that a wireless device can be inactive before a session, and in the **Idle** "post" field, key in the number of minutes that a wireless device can be inactive after a session.

In the **Session** area, key in the absolute time limit of a session (0 = no limit).

Identify the Altitude AP radios that will be assigned to this WM-AD

5 From the displayed list of **Altitude AP Radios** that are available throughout the network, check the ones to be assigned to this WM-AD.

NOTE

If two Summit WM-Series Switches have been paired for availability (as described in the Availability topic), each Summit WM-Series Switch's registered Altitude APs will appear as "foreign" in the list of available Altitude APs on the other Summit WM-Series Switch.

Once you have assigned a Altitude AP radio to four WM-ADs, it will not appear in the list for another WM-AD setup.

You can view the WM-ADs that each radio is participating in by clicking on each radio tab in the *Altitude AP Configuration* screen.

Enable Management Traffic on this WM-AD

6 To use this WM-AD for Management Traffic such as SSH, HTTPS, or SNMP, click the **Allow mgmt traffic** checkbox on. Use this capability with caution, since it overrides the built-in exception filters that prohibit such traffic on the Summit WM-Series Switch data interfaces. (See also "Port-based exception filters: built-in" on page 39.)

Enable Third Party Access Points on this WM-AD

7 If this WM-AD is to be used for third-party access points, click the **Use 3rd Party AP** checkbox on. The screen changes to include fields to enter the IP Address and MAC Address of the third-party access point. Use this function as part of the process defined in Chapter 9.

Define a next hop route for this WM-AD

8 To define a static route specifically for this WM-AD, in the **Next Hop Address** field, key in the IP address of the next hop router on the network through which you wish all traffic on this WM-AD to be directed. If traffic from a wireless device on this WM-AD is destined outside of the WM-AD, then it is forwarded to the next hop IP address, where this router applies policy and forwards the traffic. This features applies to unicast traffic only.

You can also modify the **OSPF Route Cost**.

9 To **disable OSPF Advertisement** on this WM-AD, click the checkbox on.

Set the IP address for the WM-AD (for the DHCP server on the Summit WM-Series Switch)

10 In the **Gateway** box, key in the network IP address for the WM-AD.

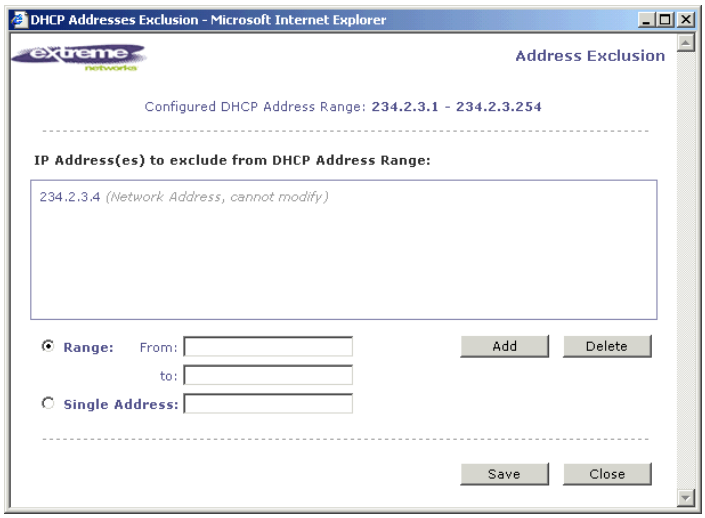
This IP address is the *default gateway* for the WM-AD. The Summit WM-Series Switch advertises this address to the wireless devices when they sign on.

11 In the **Mask** box, key in the appropriate subnet mask for this IP address, to separate the network portion from the host portion of the address (typically 255.255.255.0)

The **Address Ranges** fields populate automatically (based on the IP address you keyed in) with the range of IP addresses to be assigned to wireless devices using this WM-AD.

12 To modify the **Address Ranges**, key the first available address in the **from** box. Key the last available address in the **to** box.

13 If there are specific IP addresses to be excluded from this range, click on the **Exclusions** button. The *Address Exclusion* subscreen appears.



14 In the *Exclusions* subscreen, key in the IP addresses or address ranges to exclude. Click on the **Add** button after each entry. Click on the **Save** button to save the changes and return to the *Topology* screen.

15 The **Broadcast Address** field populates automatically, based on the Gateway IP address and subnet mask of the WM-AD. Modify this if appropriate.

16 In the **Domain Name** box, key in the external enterprise domain name.

Set time limits for IP assignments

17 In the **Default Lease** box, accept the default value of 36000 seconds (10 hours), or modify. This is the default time limit that an IP address would be assigned by the DHCP server to a wireless device.

In the **Max Lease** box, accept the default value is 2592000 seconds (720 hours, 30 days), or modify. This is the maximum time that an IP address can be assigned.

Set the name server configuration

18 In the **DNS Servers** box, key in the IP Address of the Domain Name Server(s) to be used.

19 If the DHCP server uses WINS (Windows Internet Naming Service), key in the IP address in the **WINS** box. If not, leave it blank.

Use DHCP Relay for the WM-AD

20 To use an external DHCP server, click the **Use DHCP Relay** checkbox on. The DHCP Settings area of the screen changes to display only the Gateway IP, Mask and DHCP Server fields. Key in the appropriate IP addresses and mask to reach the enterprise's external DHCP server.

Use **DHCP Relay** to force the Summit WM-Series Switch to forward DHCP requests to an external DHCP server on the enterprise network. This function will bypass the local DHCP server on Summit WM-Series Switch (to bypass steps 10 to 19 above). This function allows the enterprise to manage IP address allocation to a WM-AD from its existing infrastructure.

The range of IP addresses to be assigned to the wireless device users on this WM-AD should also be designated on the external DHCP server.

Save the new WM-AD

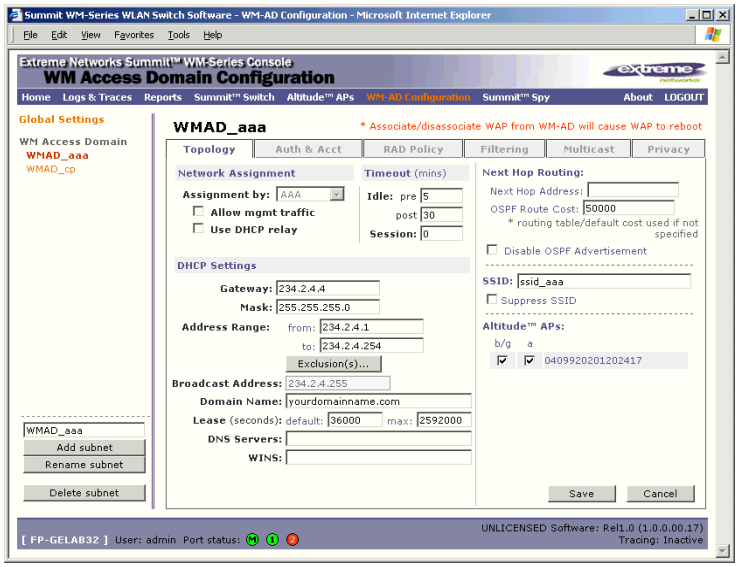
21 To save this WM-AD configuration, click on the **Save** button.

When the new Topology has been saved, the screen changes to display tabs for **Authentication and Accounting, RAD Policy**, **Filtering, Multicast** and **Privacy**.

Topology for a WM-AD for AAA

For a WM-AD with 802.1x authentication, select Network Assignment by AAA (Authentication, Authorization, Accounting) in the *Topology* screen.

In the *WM Acess Domain Configuration* screen, highlight the WM-AD name in the left-hand list and click on the **Topology** tab.



Create an AAA topology

1 Using the **Assignment by drop-down** list, select **AAA**.

2 To configure the WM-AD, follow steps 2 to 20 above, for the Topology for Captive Portal (SSID network assignment), with the exception of step 7.

Configuring a WM-AD for Third-party APs is only available with SSID network assignment.

Save the new WM-AD

3 To save this WM-AD configuration for AAA, click on the **Save** button.

Authentication for a WM-AD

The next step in configuring a WM-AD is to set up the Authentication mechanism in the *Authentication and Accounting* screen. There are various combinations available:

- If network assignment is by **SSID**, authentication can be:
  - none
  - by Captive Portal using internal Captive Portal
  - by MAC-based authentication
- If network assignment is by **AAA (802.1x)**, authentication can be:
  - by 802.1x authentication, the wireless device user must be authenticated before gaining network access
  - by MAC-based authentication

The first step for any type of authentication is to select RADIUS servers (defined in the *Global Settings* screen), to be used for:

- Authentication
- Accounting
- MAC-based authentication

MAC-based authentication enables network access to be restricted to specific devices by MAC address. The Summit WM-Series Switch queries a RADIUS server for MAC address when a wireless client attempts to connect to the network. This is available in addition to the other types of authentication for all WM-AD definitions.

The chart below shows the authentication and accounting combinations available:

Table 4: Authentication types and features

	Accounting	CDR	Internal CP
SSID / None	Unavailable	Unavailable	Unavailable
SSID / MAC	Unavailable	Unavailable	Unavailable
SSID / Int. Auth	Configurable	Configurable	Configurable
SSID / Ext. Auth	Configurable if ExtCP=T	Configurable if ExtCP=T	Unavailable
SSID / MAC / Int Auth	Configurable	Configurable	Configurable
SSID / MAC / Ext Auth	Configurable if ExtCP=T	Configurable if ExtCP=T	Unavailable
AAA	Configurable	Configurable	Unavailable
AAA / MAC	Configurable	Configurable	Unavailable

Vendor Specific Attributes (VSAs)

In addition to the standard RADIUS message, you can include Vendor Specific Attributes (VSAs). The Summit WM-Series Switch Software authentication mechanism provides six Vendor Specific Attributes (VSAs), for RADIUS and other authentication mechanisms.

Table 5: Vendor Specific Attributes in RADIUS

VSA Attribute Name	Attribute #	Comment
AP-Name	1	Name of Altitude AP as specified in the *AP Properties* screen
AP-Serial	2	Altitude AP Serial number from manufacturing
AP-Radio	3	The Altitude AP radio type the client has connected to
WM-AD-Name	4	The WM-AD that the user associated with
SSID	5	Value of SSID that the user associated with
URL-Redirection	6	Provides the specific URL that the user will be redirected to

The first five of these VSAs provide information about the identify of the specific Altitude AP that is handling the wireless device, enabling the provision of *location-based services*.

The RADIUS message also includes RADIUS attributes “Called-Station-Id” and “Calling-Station-Id” in order to include the MAC address of the wireless device.

Authentication for a WM-AD for Captive Portal

For Captive Portal authentication, the wireless device connects to the network, but can only access the specific network destinations defined in the *Non-Authenticated Filter* (see “The non-authenticated filter for Captive Portal” on page 87). One of these destinations should be a server (internal) that presents a web page logon screen (the Captive Portal). The wireless device user must input an ID and a Password. This request for authentication is sent by the Summit WM-Series Switch to a RADIUS server or other authentication server. Based on the permissions returned from the authentication server, the Summit WM-Series Switch implements policy and allows the appropriate network access.

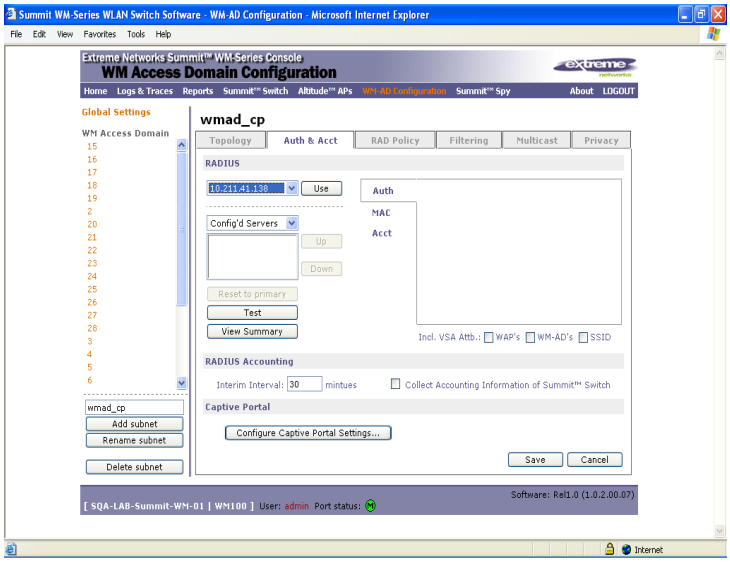
There are three mechanisms by which Captive Portal authentication can be carried out:

- internal Captive Portal: the Summit WM-Series Switch presents the Captive Portal webpage, carries out the authentication and implements policy

Captive Portal authentication relies on a RADIUS server on the enterprise network.

Set up authentication by Captive Portal

1 In the *WM Access Domain Configuration* screen, highlight the WM-AD name and click on the **Auth & Acct** tab. The *Authentication and Accounting* screen appears (in the Captive Portal version if network assignment is by SSID).

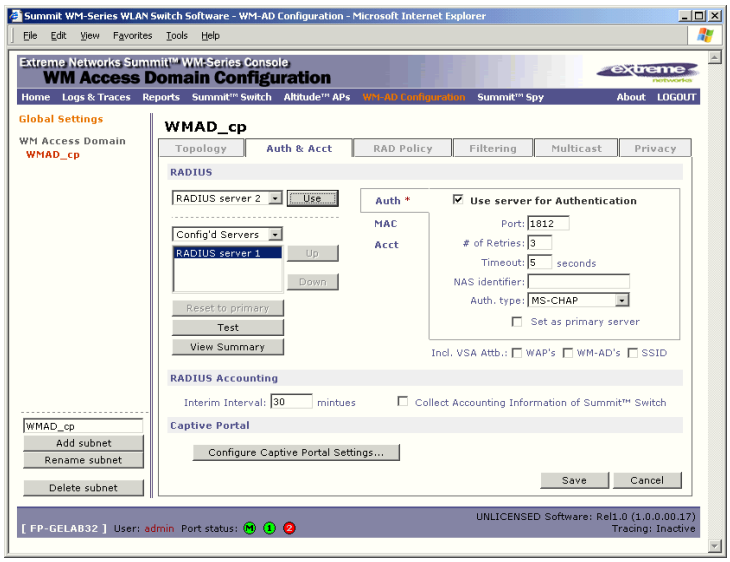


2 In the right-hand portion of the screen, there are three options:

- **Auth**. to define authentication servers
- **MAC** to define servers for MAC-based authentication
- **Acct**. to define accounting servers

Select **Auth**. A box appears around this area of the screen.

3 From the drop-down list of RADIUS servers that were defined in the *Global Settings* screen, select the server you wish to use for Captive Portal authentication. Click on the **Use** button. The boxed area fills with fields displaying the default information about this server.



This server is no longer available in the drop-down list.

The server name now appears in the list of configured servers (beside the **Up** and **Down** buttons) where it can be prioritized for RADIUS redundancy. It can also be assigned again for MAC-based authentication or accounting purposes.

A red asterisk appears in the right-hand list, showing that a server has been assigned.

4 Fill in the following fields:

Port #	The port used to access the RADIUS server (default: 1812)
# of Retries	Number of times the Summit WM-Series Switch will attempt to access the RADIUS server
Timeout	The maximum time that a Summit WM-Series Switch will wait for a response from the RADIUS server before attempting again
NAS Identifier	Network Access Server (NAS) identifier, a RADIUS attribute that identifies the server responsible for passing information to designated RADIUS Servers and then acting on the response returned. [Optional]

5 In the **Auth. Type** field, select the authentication protocol to be used by the RADIUS server to authenticate the wireless device users (for a WM-AD with Captive Portal authentication).

PAP	(Password Authentication Protocol)
CHAP	(Challenge Handshake Authentication Protocol)
MS CHAP	(Windows-specific version of CHAP)
MS CHAP v2	(Windows-specific version of CHAP, version 2)

6 In the **Include VSA Attributes** area, click on the appropriate checkbox to include the Vendor Specific Attributes in the message to the RADIUS server: **AP Identification**, **WM-AD Identification**, and **SSID Identification**.

The Vendor Specific Attributes must be defined on the RADIUS Server.

7 If appropriate, click the **Set as primary server** checkbox on.

8 To save this configuration, click on **Save**.

NOTE

*If you have already assigned a server to either MAC-based authentication or accounting, and wish to use it again for authentication, highlight its name in the list beside the **Up** and **Down** buttons. Click the **Use server for Authentication** checkbox on. The boxed area populates with fields about this server.*

Define the RADIUS server priority for RADIUS redundancy

If more than one server has been defined for any type of authentication, you can define the priority of the servers in the case of failover.

1 Select from the drop-down list: Configured Servers, Authentication Servers, MAC Servers, Accounting Servers.

2 Highlight a RADIUS server in the list and use the **Up** or **Down** key to change the order.

The first server in the list is the active one. In the event of a failover of the main RADIUS server (if no response after the set number of retries), then the other servers in the list will be polled on a round-robin basis until one responds.

If one of the other servers becomes the active one during a failover, an "A" will appear after that server name.

If all defined RADIUS servers fail to respond, a critical message is generated in the logs.

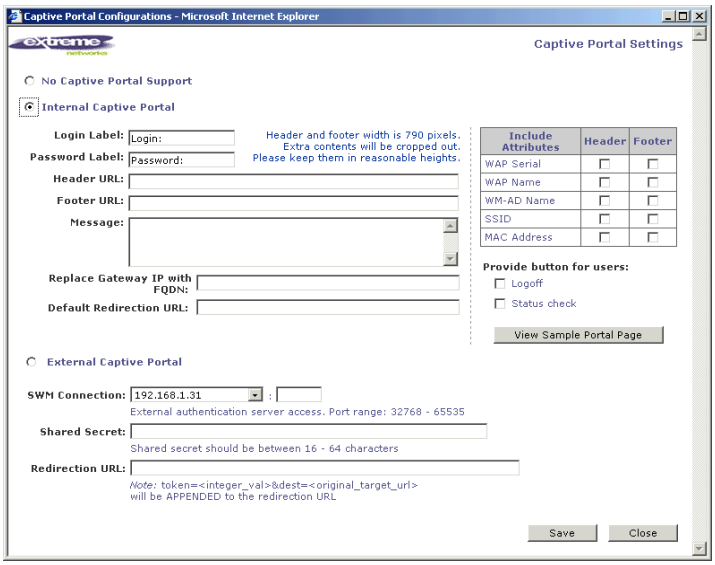
3 To run a test of the Summit WM-Series Switch's connection to all configured RADIUS servers, click on the **Test** button. In the pop-up screen, key in your **User ID** and click on the **Test** button.

4 To view a summary of the RADIUS test results, click on the **View Summary** button.

5 To save the authentication parameters for this WM-AD, click on the **Save** button.

Configure Captive Portal for internal authentication

Click on the **Configure Captive Settings** button in the *Authentication* screen. The Captive Portal Settings subscreen appears.



On the Captive Portal Settings subscreen, you have three options (radio buttons):

- No Captive Portal Support
- Internal Captive Portal: define the parameters of the internal Captive Portal page presented by the Summit WM-Series Switch, and the authentication request from the Summit WM-Series Switch to the RADIUS server

Configure the Captive Portal settings for internal Captive Portal

1 Click on the **Internal Captive Portal** radio button in the Captive Portal Settings screen.

2 Key in the text that will appear on the Captive Portal page.

Login Label	The text that will appear as a label for the user login field
Password Label	The text that will appear as a label for the user password field

3 Key in the locations of the header and footers.

Header URL	The location of the file to be displayed in the Header portion of the Captive Portal screen. This page can be customized to suit your company, with logos or other graphics. (Caution: Ensure that such graphics in the header are not so large that they push the login area out of view.)
Footer URL	The location of the file to be displayed in the Footer portion of the Captive Portal screen

4 In the **Message** field, key in the message that will appear above the login field to greet the user. For example, this could explain why this Captive Portal page is appearing, and what the user should do.

5 If use a Fully Qualified Domain Name (FQDN) as the gateway address, key in the appropriate name in the **Replace Gateway IP with FQDN** field.

6 Key in the **Default Redirection URL**.

7 Click on the appropriate checkboxes to include the following VSA Attributes in the message to the authentication server: AP Serial number, AP Name, WM-AD Name, SSID, MAC Address. Check whether these apply to the header or footer of the Captive Portal page.

These choices influence what URL is returned in either area. For example, wireless users can be identified by which Altitude AP or which WM-AD they are associated with, and can be presented with a Captive Portal web page that is customized for those identifiers.

Refer to a separate Technical Note for instructions on integrating the VSA information into Captive Portal authentication display.

8 To provide either of two buttons on a popup status page, click the appropriate checkbox on:

- **Logoff**, for a button that displays a popup logoff screen, allowing users to control their logoff
- **Status check**, for a button that displays a popup window with session statistics for users to monitor their usage and time left in session.

9 To save this configuration, click on **Save**.

10 To see how the Captive Portal page you have designed will look (after saving the configuration), click on the **View Sample Portal Page** button.

NOTE

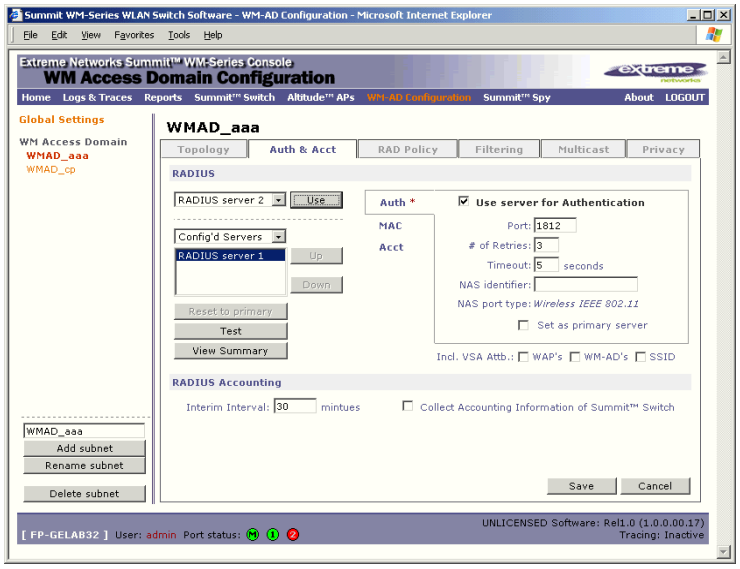
In order for Captive Portal authentication to work, all the URLs referenced in the Captive Portal setup must also be specifically identified and allowed in the Non-Authenticated Filter (see "The non-authenticated filter for Captive Portal" on page 87).

Authentication for a WM-AD for AAA

Set up authentication by AAA (802.1x) method

1 In the *WM Access Domain Configuration* screen, highlight the WM-AD name and click on the **Auth & Acct** tab. For an AAA WM-AD, the AAA version of the *Authentication* screen appears.

2 Follow steps 2 to 10 described above for Captive Portal, except for Step 5 (Authentication Type) which does not apply to AAA. See "Authentication for a WM-AD for Captive Portal" on page 77.



3 To save the authentication parameters for this WM-AD, click on the **Save** button.

MAC-based authentication for a WM-AD

MAC-based authentication enables network access to be restricted to specific devices by MAC address. The Summit WM-Series Switch queries a RADIUS server for MAC address when a wireless client attempts to connect to the network.

MAC-based authentication can be set up on any type of WM-AD, in addition to the Captive Portal or AAA authentication.

To set up a RADIUS server for MAC-based authentication, you must set up a user account with UserID=MAC and Password=MAC for each user.

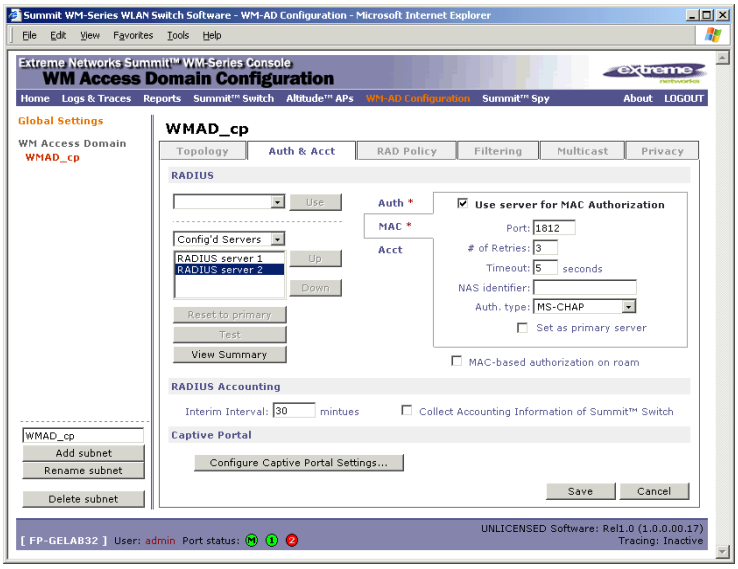
If MAC-based authentication is to be used in conjunction with the 802.1x or Captive Portal authentication, an additional account with a real "UserID" and "Password" must also be set up on the RADIUS server.

Define MAC-based authentication for a WM-AD

1 In the *WM Access Domain Configuration* screen, highlight the WM-AD name and click on the **Auth & Acct** tab. The *Authentication and Accounting* screen appears (in either Captive Portal or AAA versions depending on network assignment). In the right-hand portion of the screen, select **MAC**. A box appears around this area of the screen.

2 From the drop-down list of RADIUS servers defined in the *Global Settings* screen, select the server you wish to use for MAC-based authentication. Click on the **Use** button.

The boxed area fills with fields displaying the default information about this server.



Alternatively, highlight a server name that has already been used for another type of authentication, or accounting, and click on the checkbox **User server for MAC Authentication.**

3 Fill in the fields described above for Captive Portal authentication or for AAA authentication.

4 In the **Auth. Type** field, select the authentication protocol to be used by the RADIUS server to authenticate the wireless device users (for a Captive Portal WM-AD), as described above for Captive Portal authentication.

5 In the **Include VSA Attributes** area, click on the appropriate checkbox to include the Vendor Specific Attributes in the message to the RADIUS server: **AP Identification**, **WM-AD Identification**, and **SSID Identification**.

The Vendor Specific Attributes must be defined on the RADIUS Server.

6 To enable **MAC-based authentication on roam**, click the checkbox on.

7 To save these authentication parameters for this WM-AD, click on the **Save** button.

Accounting for a WM-AD

The next step is to enable and configure, for a WM-AD, the methods of accounting to track the activity of a wireless device users. Two types of accounting can be enabled:

- Summit WM-Series Switch Accounting: enables the Summit WM-Series Switch to generate Call Data Records (CDRs) in a flat file on the Summit WM-Series Switch
- RADIUS Accounting: enables the Summit WM-Series Switch to generate an "accounting request packet" with an "accounting start record" after successful login by the wireless device user and an "accounting stop record" based on session termination. The Summit WM-Series Switch sends the accounting requests to a remote RADIUS server.

Summit WM-Series Switch Accounting creates Call Data Records (CDRs) in a standard format of user session information, such as start time and duration of session. The CDRs are stored in flat files that be downloaded via the CLI.

If you enable RADIUS Accounting, you need to specify a RADIUS accounting server.

Enable and configure accounting methods for this WM-AD

1 In the *WM Access Domain Configuration* screen, click on the **Auth & Acct** tab. The *Authentication* screen appears, for the highlighted WM-AD.

2 In the **RADIUS Accounting** area of the screen, to enable Summit WM-Series Switch Accounting, click the **Collect Accounting Information** checkbox on.

3 From the drop-down list of RADIUS servers that were defined in the *Global Settings* screen, select the server you wish to use for RADIUS accounting. Click on the **Use** button.

The **Acct.** portion of the screen displays the information about this server, and it is no longer available in the list.

4 Click the **Use server for Accounting** checkbox on.

5 Fill in the fields as described above for the Authentication server.

6 Type in the **RADIUS Accounting Interim Interval**. Interim accounting records are sent out if the interim time interval is reached before the session ends. The default is 60 minutes.

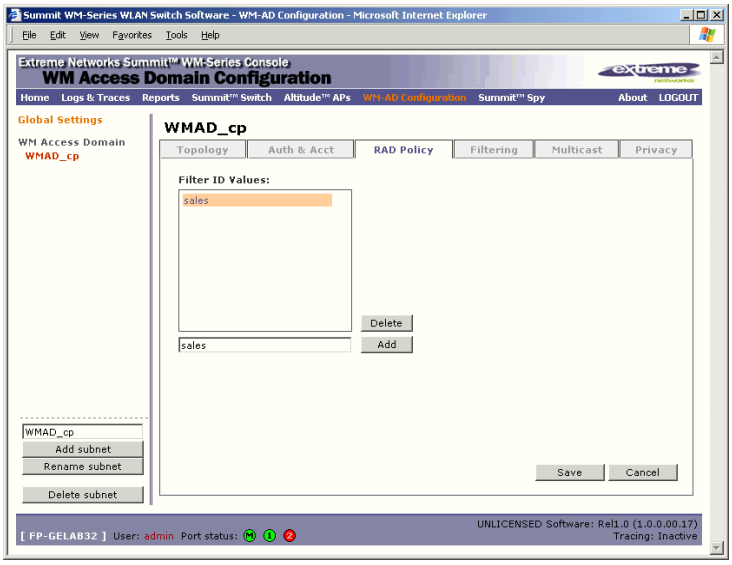
7 To save this configuration, click on **Save**.

RADIUS Policy for a WM-AD

The next step is to define the Filter ID values for a WM-AD. These Filter ID values must match those set up on the RADIUS servers.

RADIUS Policy for Captive Portal

1 In the *WM Access Domain Configuration* screen, highlight the WM-AD name and click on the **RAD Policy** tab. For a WM-AD with SSID network assignment, the Captive Portal version of the *RADIUS Policy* screen appears.



Define the Filter ID values on this WM-AD.

1 In the **Filter ID Values** entry field, key in the name of a group that you want to define specific filtering rules for, to control network access. Click on the **Add** button. The Filter ID value appears in the list above.

Repeat for additional Filter ID values.

These will appear in the Filter ID list in the *Filtering* screen. These Filter ID values must match the those set up for the Filter-ID attribute in the RADIUS server.

2 To save the Filter ID values for this WM-AD, click on the **Save** button.

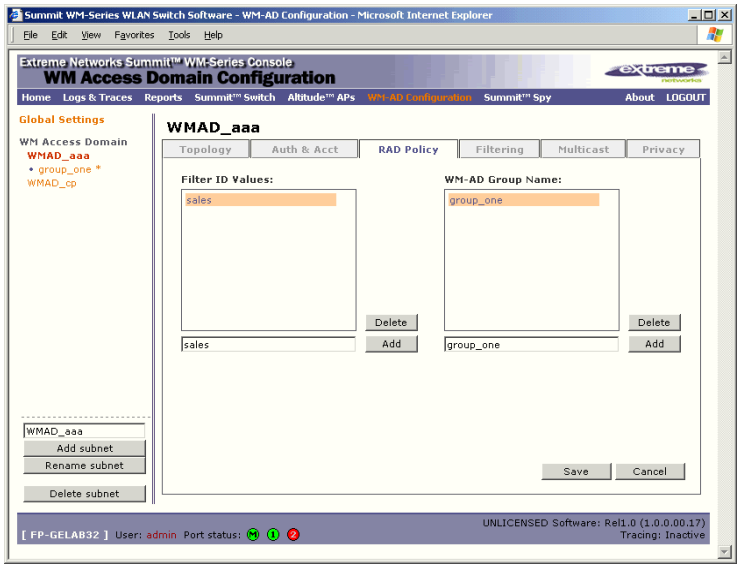
RADIUS Policy for AAA and AAA groups

In addition the Filter ID values described above, you can also set up group ID, for a WM-AD with AAA authentication. You can set up a group within a WM-AD that relies on the RADIUS attribute Login-LAT-Group (RFC2865). For each group, you can define filtering rules to control access to the network.

If you define a group within an AAA WM-AD, the group (or child) definition acquires the same authentication and privacy parameters as the parent WM-AD. However, you need to define a different topology and filtering rules for this group.

Define the Filter ID values on this WM-AD

1 In the *WM Access Domain Configuration* screen, highlight the WM-AD name and click on the **RAD Policy** tab. For a WM-AD with AAA network assignment, the AAA version of the *RADIUS Policy* screen appears.



2 In the **Filter ID Values** entry field, key in the name of a group that you want to define specific filtering rules for, to control network access. Click on the **Add** button. The Filter ID value appears in the list above. Repeat for additional Filter ID values.

These will appear in the Filter ID list in the *Filtering* screen. These Filter ID values must match the those set up for the Filter-ID attribute in the RADIUS server.

3 To create and define a WM-AD Group within the selected parent WM-AD, key in the name in the **WM-AD Group Name** field. Then click on the **Add** button.

The Group Name will appear as a child of the parent WM-AD in the left-hand list.

4 To save the Filter ID values and Group definition for this WM-AD, click on the **Save** button.

Filtering rules for a WM-AD

The next step is to configure the filtering rules for a WM-AD. Four types of filters are applied by the Summit WM-Series Switch in the following order:

1 Exception filter, to provide the administrator optional additional flexibility in securing the system and blocking Denial of Service (DoS) attacks, on any type of WM-AD.

2 Non-Authenticated filter, with restrictive filtering rules that apply before authentication, to control network access and to direct users to a Captive Portal web page for login.

3 Group filters (by Filter ID) for designated user groups, that apply after authentication, when the RADIUS server returns the “access-accept” message along with the Filter-ID attribute value associated with the user.

4 Default filter, to control access if there is no matching Filter ID for a user.

For an AAA WM-AD, since users have already been authenticated, there is no need for a Non-Authenticated filter. When authentication is returned, then the Filter ID group filters are applied. For AAA, a WM-AD can have a subgoup with Login-LAT-group ID that has its own filtering rules. If no Filter ID matches are found, then the Default filter is applied.

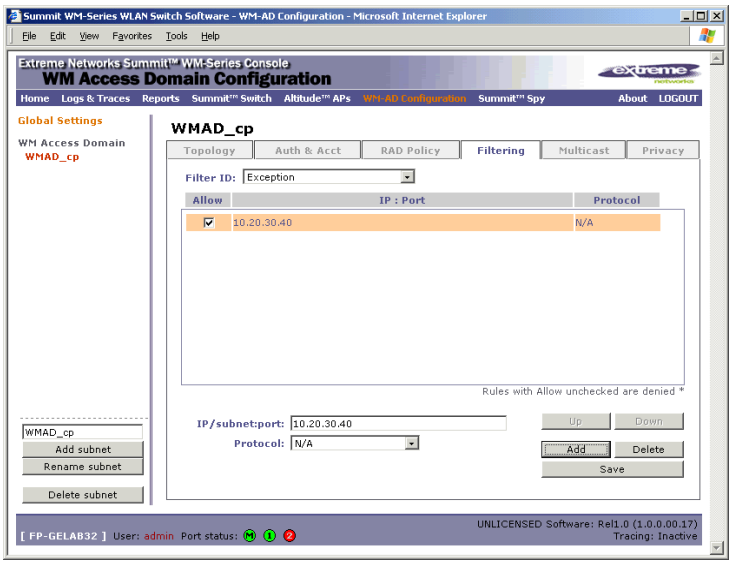
Filtering rules for an exception filter

The exception filter on an WM-AD applies only to the destination portion of the packet. The screen is set to allow or deny (allow left unchecked) traffic to the specified IP address and IP port.

Adding the exception filtering rules allows the network administration to either tighten or relax the built-in filtering that automatically drops packets not specifically allowed by filtering rule definitions. The exception filtering rules could deny access in the event of DoS attack, or on the other hand, could allow certain types of management traffic that would otherwise be denied.

Define the filtering rules for an exception filter

1 In the *WM Access Domain Configuration - Filtering* screen, using the **Filter ID** drop-down list, select **Exception**.


Summit WM-Series WLAN Switch Software - WM-AD Configuration - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Extreme Networks Summit™ WM-Series Console
WM Access Domain Configuration
Home Logs & Traces Reports Summit™ Switch Altitude™ APs WM-AD Configuration Summit™ Spy About LOGOUT
Global Settings
WM Access Domain
WMAD_cp
WMAD_cp
Topology Auth & Acct RAD Policy Filtering Multicast Privacy
Filter ID: Exception
Allow IP : Port Protocol
10.20.30.40 N/A
Rules with Allow unchecked are denied *
IP/subnet:port: 10.20.30.40
Protocol: N/A
Up Down
Add Delete
Save
WMAD_cp
Add subnet
Rename subnet
Delete subnet
[FP-GELAB32] User: admin Port status:
UNLICENSED Software: Rel1.0 (1.0.0.00.17)
Tracing: Inactive

2 Follow the steps described below for the non-authenticated filter.

The non-authenticated filter for Captive Portal

The non-authenticated filter should allow access to the Captive Portal page IP address, as well as to any URLs for the header and footer of the Captive Portal page. The filter should also allow network access to the IP address of the DNS server and to the Network Address, the Gateway, of the WM-AD (the WM-AD Gateway is used as the IP for the Captive Portal page).

You can also set up filtering rules to allow access, before authentication, to explicitly defined areas of the network. Then you must deny all other access.

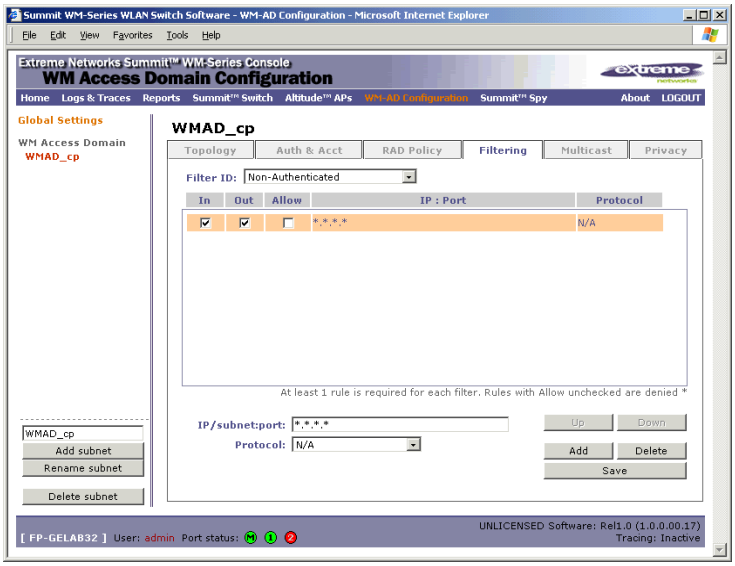
Redirection and Captive Portal credentials apply to HTTP traffic only. A wireless device user attempting to reach websites other than those specifically allowed in the Non-Authenticated Filter will be redirected to the allowed destinations. Most HTTP traffic outside of those defined in the non-authenticated filter will be redirected.

All other network access will be controlled after the user is authenticated, when the filter ID or default filtering rules are applied. The wireless device user who does not authenticate will not get a wireless session.

Define filtering rules for a non-authenticated filter

1 In the *WM Access Domain Configuration* screen, highlight the WM-AD name and click on the **Filtering** tab. For a WM-AD with SSID network assignment, the Captive Portal version of the *Filtering* screen appears.

2 Using the **Filter ID** drop-down list, select **Non-Authenticated**.


Summit WM-Series WLAN Switch Software - WM-AD Configuration - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Extreme Networks Summit™ WM-Series Console
WM Access Domain Configuration
Home Logs & Traces Reports Summit™ Switch Altitude™ APs WM-AD Configuration Summit™ Spy About LOGOUT
Global Settings
WM Access Domain
WMAD_cp
WMAD_cp
Topology Auth & Acct RAD Policy Filtering Multicast Privacy
Filter ID: Non-Authenticated
In Out Allow IP : Port Protocol
..*.* N/A
At least 1 rule is required for each filter. Rules with Allow unchecked are denied *
IP/subnet:port: *.*.*.*
Protocol: N/A
Up Down
Add Delete
Save
WMAD_cp
Add subnet
Rename subnet
Delete subnet
[FP-GELAB32] User: admin Port status:
UNLICENSED Software: Rel1.0 (1.0.0.00.17)
Tracing: Inactive

The *Filtering* screen automatically provides a "Deny All" rule already in place. Use this rule as the final rule in the Non-Authenticated Filter for Captive Portal.

3 For each filtering rule you are defining:

IP / Port: Type in the destination IP address. You can also specify an IP range, a port designation or a port range on that IP address.

Protocol: Default is N/A. To specify a protocol, select from the drop-down list (may include UDP, TCP, IPsec-ESP, IPsec-AH, ICMP).

4 For Captive Portal, define a rule to allow access to the default gateway for this WM-AD. Select **IP / Port** and key in the default gateway IP address that you defined in the *Topology* screen for this WM-AD.

5 Click on the **Add** button. The information appears in a new line in the **Filter Rules** area of the screen.

6 Highlight the new filtering rule and fill in (or leave unchecked) the three checkboxes in the combinations that define the traffic access:

In: Click checkbox *on* to refer to traffic from the wireless device that is trying to get on the network ("going to" the network)

Out: Click checkbox *on* to refer to traffic from the network host that is trying to get to a wireless device. ("coming from" the network)

Allow: Click checkbox *on* to *allow*. Leave unchecked to *disallow*.

For Captive Portal, to allow access to the defined IP address, check all three boxes on.

7 Edit the order of a filtering rule by highlighting the line and clicking on the **Up** and **Down** buttons. The filtering rules are executed in the order defined here.

8 To save the filtering rules, click on the **Save** button.

Non-authenticated filters: examples

A basic Non-Authenticated filter for Captive Portal should have three rules in this order:

In	Out	Allow	IP / Port	Description
x	x	x	IP address of the Default Gateway	Allow all incoming wireless devices access to the default gateway of the WM-AD.
x	x	x	IP address of the DNS Server	Allow all incoming wireless devices access to the DNS server of the WM-AD.
x	x		*.*.*.*	Deny everything else.

If you put URLs in the header and footer of the Captive Portal page, you must include a filtering rule to allow traffic to each of these URLs. Put these rules above the "deny everything" rule.

Here is another example of a Non-Authenticated Filter that adds two more filtering rules: one denies access to a specific IP address, and the next rule allows only HTTP traffic, before denying all other access:

In	Out	Allow	IP / Port	Description
x	x	x	IP address of the Default Gateway	Allow all incoming wireless devices access to the default gateway of the WM-AD.
x	x	x	IP address of the DNS Server	Allow all incoming wireless devices access to the DNS server of the WM-AD.
x	x		[a specific IP address, or address plus range]	Deny all traffic to a specific IP address, or to a specific IP address range (such as :0/24).
x	x	x	*.*.*.*:80	Allow all port 80 (HTTP) traffic.
x	x		*.*.*.*	Deny everything else.

Once a wireless device user has logged in on the Captive Portal page, and has been authenticated by the RADIUS server, then the following filters will apply:

- Filter ID Filter, if a Filter ID associated with this user was returned the authentication server
- Default Filter, if no matching Filter ID was returned from the authentication server

These filters are described below.

Filtering rules for a Filter ID group

The next step is to define the filtering rules for the Filter ID values on the WM-AD.

When the wireless device user enters a login identification, that identification is sent by the Summit WM-Series Switch to the RADIUS server or other authentication server, through a sequence of exchanges depending on the type of authentication protocol used.

When the server allows this request for authentication (sends an “access-accept” message), the RADIUS server may also send back to the Summit WM-Series Switch a Filter ID attribute value associated with the user. For an AAA WM-AD, a Login-LAT-Group identifier for the user may also be returned.

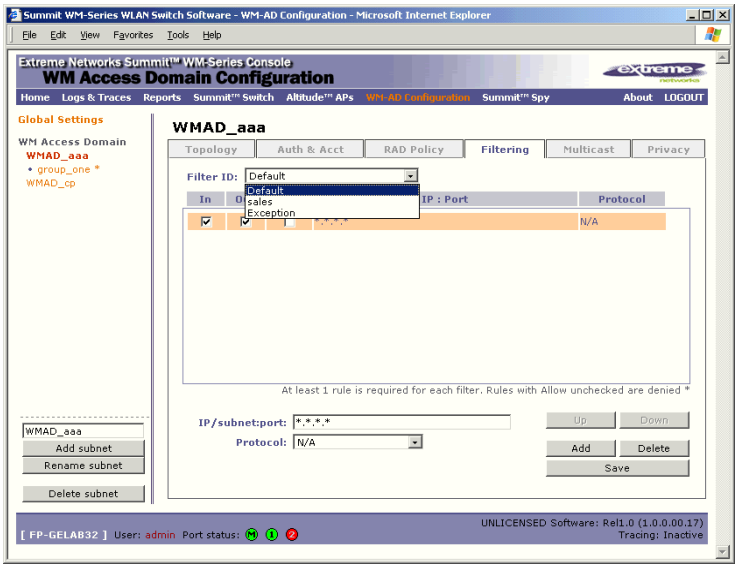
If the Filter ID attribute value (or Login-LAT-Group attribute value) from the RADIUS server matches a Filter ID value that you have set up on the Summit WM-Series Switch, the Summit WM-Series Switch applies to the wireless device user the filtering rules that you defined for that Filter ID value.

If no Filter ID is returned by the authentication server, or no match is found on the Summit WM-Series Switch, then the filtering rules in the Default Filter will apply to the wireless device user.

Define filtering rules for a Filter ID group

1 In the *WM Access Domain Configuration* screen, click on the **Filtering** tab. The *Filtering* screen appears for the highlighted WM-AD.

2 Using the **Filter ID** drop-down list, select one of the names you defined in the **Filter ID Values** field in the *Authentication* screen [one of your enterprise's user groups, such as Sales, Engineering, Teacher, Guest....]



The screen automatically provides a “Deny All” rule already in place. This can be modified to “Allow All”, if appropriate to the network access needs for this WM-AD.

3 Select one of the following as the basis for each filtering rule you are defining:

IP / Port: Type in the destination IP address, and if desired, the port designation on that IP address.

Protocol: Select from the drop-down list (may include UDP, TCP, IPsec-ESP, IPsec-AH, ICMP)

4 Click on the **Add** button. The information appears in a new line in the **Filter Rules** area of the screen.

5 Highlight the new filtering rule and fill in (or leave unchecked) the three checkboxes in the combinations that define the traffic access:

In: Click checkbox on to refer to traffic from the wireless device that is trying to get on the network (“going to” to network)

Out: Click checkbox on to refer to traffic from the network host that is trying to get to a wireless device. (“coming from” the network)

Allow: Click checkbox on to allow. Leave unchecked to disallow

6 Edit the order of a filtering rule by highlighting the line and clicking on the **Up** and **Down** buttons. The filtering rules are executed in the order defined here

7 To save the filtering rules, click on the **Save** button.

Filtering Rules by Filter ID: Examples

Below are two examples of possible filtering rules for a Filter ID. The first disallows only some specific access before allowing everything else.

In	Out	Allow	IP / Port	Description
x	x		*.*.*.*:22-23	Deny all telnet sessions
x	x		[specific IP address, range]	Deny all traffic to a specific IP address or address range
x	x	x	*.*.*.*.	Allow everything else

The second example does the opposite of the first example. It allows only some specific access and denies everything else.

In	Out	Allow	IP / Port	Description
x	x	x	[specific IP address, range]	Allow traffic to a specific IP address or address range.
x	x		*.*.*.*.	Deny everything else.

Filtering rules for a default filter

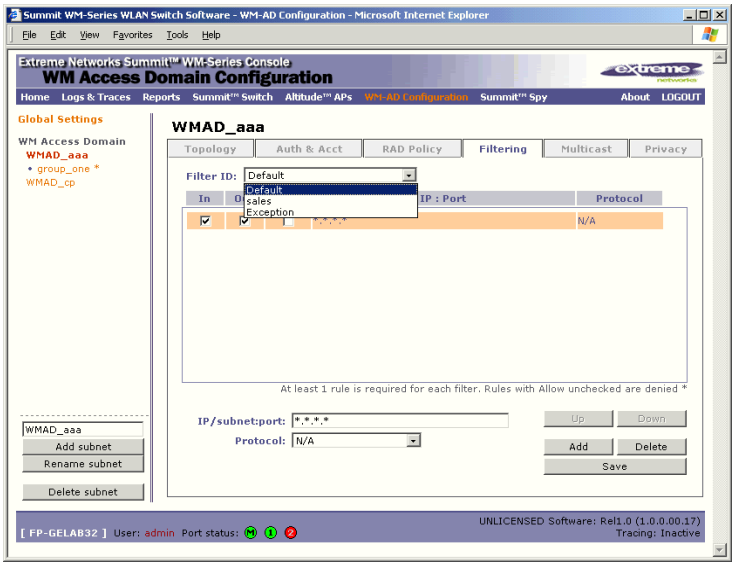
After authentication of the wireless device user, the default filter will apply only after:

- no match is found for the Exception flittering rules
- no Filter ID attribute value is returned by the authentication server for this user
- no match is found on the Summit WM-Series Switch for a Filter ID value

The final rule in the Default filter should be a catch-all for any traffic that did not match a filter. A final “allow all” rule in a Default Filter will ensure that a packet is not dropped entirely if no other match can be found.

Define the filtering rules for a default filter

1 In the *WM Access Domain Configuration - Filtering* screen, using the **Filter ID** drop-down list, select **Default**.



2 Follow Steps 2 to 6, as described above for Filter ID values rules.

3 To save the filtering rules, click on the **Save** button.

Default Filter: Examples

Here is an example of filtering rules for a Default Filter:

In	Out	Allow	IP / Port	Description
x	x		Intranet IP, range	Deny all access to an IP range
x	x		Port 80 (HTTP)	Deny all access to web browsing
x	x		Intranet IP	Deny all access to a specific IP
x	x	x	*.*.*.*.	Allow everything else

Here is another example of filtering rules for a Default Filter:

In	Out	Allow	IP / Port	Description
x			Port 80 (HTTP) on host IP	Deny all incoming wireless devices access to web browsing the host
	x		Intranet IP 10.3.0.20, ports 10-30	Deny all traffic from the network to the wireless devices on the port range, such as TELNET (port 23) or FTP (port 21)
x		x	Intranet IP 10.3.0.20	Allow all other traffic from the wireless devices to the Intranet network
	x	x	Intranet IP 10.3.0.20	Allow all other traffic from Intranet network to wireless devices
x	x	x	*.*.*.*.	Allow everything else

Filtering Rules for an AAA Group WM-AD

If you defined a child group for an AAA WM-AD, it will have the same authentication parameters and Filter IDs as the parent WM-AD. However, you can define different filtering rules for these Filters IDs in the child configuration than in the parent configuration.

1. In the *WM Access Domain Configuration* screen, highlight the WM-AD group name in the list and click on the Filtering tab. The Filtering screen for this WM-AD group appears.
2. Follow Steps 2 to 6, as described above for a parent WM-AD.
3. To save the filtering rules, click on the **Save** button.

Filtering rules between two wireless devices

Traffic from two wireless devices that are on the same WM-AD and are connected to the same Altitude AP will pass through the Summit WM-Series Switch and therefore be subject to filtering policy. You can set up filtering rules that allow each wireless device access to the default gateway, but prevent each device from communicating each other.

Add the following two rules to a Filter ID filter before allowing everything else:

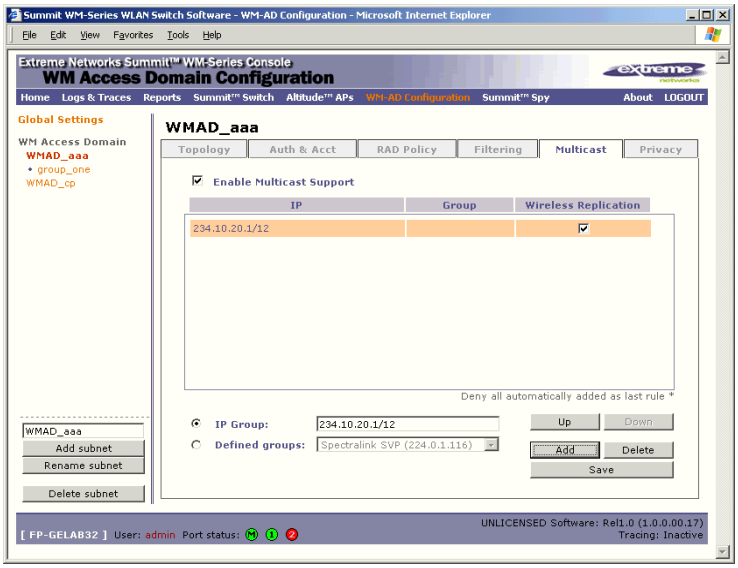
In	Out	Allow	IP / Port	Description
x	x	x	[Intranet IP]	Allow access to the Gateway IP address of the WM-AD only
x	x		[Intranet IP, range]	Deny all access to the WM-AD subnet range 0/24
x	x	x	*.*.*.*.	Allow everything else

Multicast for a WM-AD

A mechanism that supports multicast traffic can be enabled as part of a WM-AD definition. This is provided to support the demands of VoIP and IPTV network traffic, while still providing the network access control.

In the *Multicast* screen, you define a list of multicast groups whose traffic is allowed to be forwarded to and from the WM-AD. The default behavior is to drop the packets. For each group defined, you can enable Multicast Replication by group.

1 In the *WM Access Domain Configuration* screen, highlight the WM-AD name and click on the **Multicast** tab. The *Multicast* screen for this WM-AD appears.



2 To enable the multicast function, click the **Enable Multicast Support** checkbox on.

3 Define the multicast groups by clicking one of the radio buttons:

- **IP Group**: Key in the IP address range
- **Defined groups**: select from the drop-down list.

4 Click on the **Add** button. The group appears in the list above.

5 To enable the defined multicast replication for this group, click the **Wireless Replication** checkbox on.

6 To modify the priority of the multicast groups, highlight the group row and click the **Up** or **Down** buttons.

7 A "Deny all" rule is automatically added as the last rule (IP = *.*.*.* and the Replication box left unchecked). This ensures that all other traffic is dropped.

8 To save these settings, click on the **Save** button.

Privacy for a WM-AD

Privacy for a WM-AD for Captive Portal

For the Captive Portal WM-AD, there are three options for the Privacy mechanism:

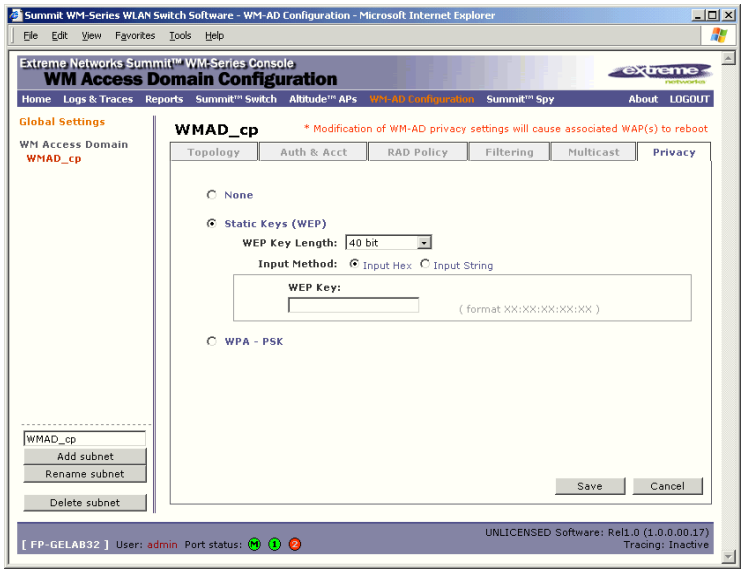
- None
- Static Wired Equivalent Privacy (WEP) keys for a selected WM-AD, so that it matches the WEP mechanism used on the rest of the network. You can assign each radio on a Altitude AP to up to four WM-ADs by SSID. For each WM-AD, only one WEP key can be specified. Summit WM-Series Switch Software always uses the first key (key index 0).
- Wi-Fi Protected Access (WPA) privacy in PSK mode, using a Pre-Shared Key (PSK), or shared secret for authentication. WPA a new security solution that adds authentication to enhanced WEP encryption and key management. WPA in PSK mode does not require an authentication server (suitable for home or small office).

Configure Privacy by static WEP for a Captive Portal WM-AD

1 In the *WM Access Domain Configuration* screen, highlight the WM-AD name and click on the **Privacy** tab. For a WM-AD with SSID network assignment, the Captive Portal version of the *Privacy* screen appears.

2 For no privacy mechanism on this WM-AD, click on the **None** radio button.

3 To configure static keys for WEP, click on the **Static Keys (WEP)** radio button.


Summit WM-Series WLAN Switch Software - WM-AD Configuration - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Extreme Networks Summit™ WM-Series Console
WM Access Domain Configuration
Home Logs & Traces Reports Summit™ Switch Altitude™ APs WM-AD Configuration Summit™ Spy About LOGOUT
Global Settings
WM Access Domain
WMAD_cp
WMAD_cp
* Modification of WM-AD privacy settings will cause associated WAP(s) to reboot
Topology Auth & Acct RAD Policy Filtering Multicast Privacy
None
Static Keys (WEP)
WEP Key Length: 40 bit
Input Method: Input Hex Input String
WEP Key:
(format XX:XX:XX:XX:XX)
WPA - PSK
WMAD_cp
Add subnet
Rename subnet
Delete subnet
Save
Cancel
[FP-GELAB32] User: admin Port status:
UNLICENSED Software: Rel1.0 (1.0.0.00.17)
Tracing: Inactive

4 From the drop-down list, select the **WEP Key Length**: 40-bit, 104-bit, 128-bit

5 Click on the appropriate radio button to select the **Input Method**: Input Hex, Input String.

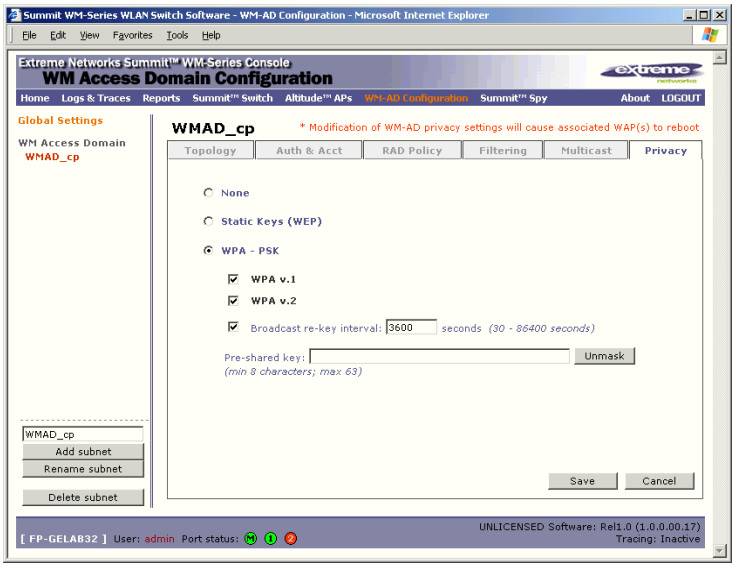
6 Type in the WEP key input, as appropriate to the technique selected. The key is generated automatically, based on the input.

7 To save these settings, click on the **Save** button.

Configure privacy by WPA-PSK for a Captive Portal WM-AD

1 In the *WM Access Domain Configuration* screen, click on the **Privacy** tab. The *Privacy* screen appears for the highlighted WM-AD.

2 To configure privacy by WPA-PSK, click on the **WPA-PSK** radio button.


Summit WM-Series WLAN Switch Software - WM-AD Configuration - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Extreme Networks Summit™ WM-Series Console
WM Access Domain Configuration
Home Logs & Traces Reports Summit™ Switch Altitude™ APs WM-AD Configuration Summit™ Spy About LOGOUT
Global Settings
WM Access Domain
WMAD_cp
WMAD_cp
* Modification of WM-AD privacy settings will cause associated WAP(s) to reboot
Topology Auth & Acct RAD Policy Filtering Multicast Privacy
None
Static Keys (WEP)
WPA - PSK
WPA v.1
WPA v.2
Broadcast re-key interval: 3600 seconds (30 - 86400 seconds)
Pre-shared key:
Unmask
(min 8 characters; max 63)
WMAD_cp
Add subnet
Rename subnet
Delete subnet
Save
Cancel
[FP-GELAB32] User: admin Port status:
UNLICENSED Software: Rel1.0 (1.0.0.00.17)
Tracing: Inactive

3 Type in the **Pre-Shared Key** (PSK), or shared secret, to be used between the wireless device and Altitude AP. The key should be between 8 and 63 characters. It is used to generate the 256-bit key.

4 To display the Pre-Shared Key (in order to proofread your entry before saving the configuration), click on the **Unmask** button. To mask the key again, click on the button again (the button toggles between **Mask** and **Unmask**).

5 To enable re-keying after a time interval, click the **Broadcast re-key interval** checkbox on (the default is on). Type in the re-key time interval (the time after which the broadcast encryption key is changed automatically) in seconds.

If the box is unchecked, the Broadcast encryption key is never changed and the Altitude AP will always use the same broadcast key for Broadcast/Multicast transmissions. Note that this reduces the level of security for wireless communications.

6 To save the privacy parameters for the new WM-AD, click on the **Save** button.

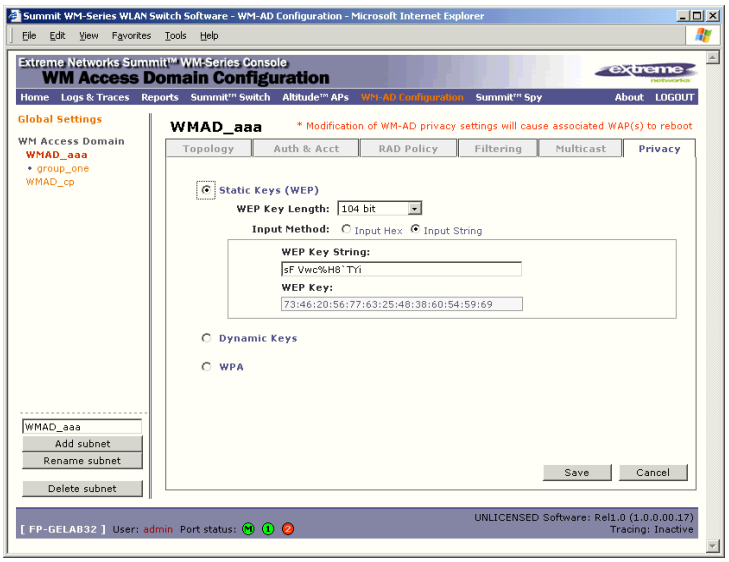
Privacy for a WM-AD for AAA

For a WM-AD with authentication by 802.1x (AAA), there are four Privacy options:

- Static keys (WEP)
- Dynamic keys
- Wi-Fi Protected Access (WPA) version 1, with encryption by Temporal Key Integrity Protocol (TKIP)
- Wi-Fi Protected Access (WPA) version 2, with encryption by Advanced Encryption Standard with Counter-Mode/CBC-MAC Protocol (AES-CCMP)

Set up static WEP privacy for a WM-AD for AAA

1 In the *WM Access Domain Configuration* screen, highlight the WM-AD name and click on the **Privacy** tab. For a AAA WM-AD, the AAA version of the *Privacy* screen appears.



2 To use static keys, click on the **Static Keys (WEP)** radio button.

3 From the drop-down list, select the **WEP Key Length**: 40-bit, 104-bit, 128 bit

4 Click on the appropriate radio button to select the **Input Method**: Input Hex, Input String.

5 Type in the WEP key input, as appropriate to the technique selected. The key is generated automatically, based on the input.

6 To save these settings, click on the **Save** button.

Set up dynamic WEP privacy for a selected AAA WM-AD

The dynamic key WEP mechanism changes to key for each user and each session.

1 To use dynamic keys, click on the **Dynamic Keys** radio button.

2 To save these settings, click on the **Save** button.

Privacy for a WM-AD for AAA: Wi-Fi Protected Access (WPA v1 and WPA v2)

The WM-AD Privacy function supports Wi-Fi Protected Access (WPA v1 and WPA v2), a security solution that adds authentication to enhanced WEP encryption and key management.

The authentication portion of WPA for AAA is in Enterprise Mode:

- Specifies 802.1x with Extensible Authentication Protocol (EAP)
- Requires a RADIUS or other authentication server
- Uses RADIUS protocols for authentication and key distribution
- Centralizes management of user credentials

The encryption portion of WPA v1 is Temporal Key Integrity Protocol (TKIP). TKIP includes:

- a per-packet key mixing function that shares a starting key between devices, and then changes their encryption key for every packet or after the specified re-key time interval.
- a extended WEP key length of 256-bits
- an enhanced Initialization Vector (IV) of 48 bits, instead of 24 bits, making it more difficult to compromise.
- a Message Integrity Check or Code (MIC), an additional 8-byte code that is inserted before the standard WEP 4-byte Integrity Check Value (ICV). These integrity codes are used to calculate and compare, between sender and receiver, the value of all bits in a message, to ensure that the message has not been tampered with.

The encryption portion of WPA v2 is Advanced Encryption Standard (AES). AES includes:

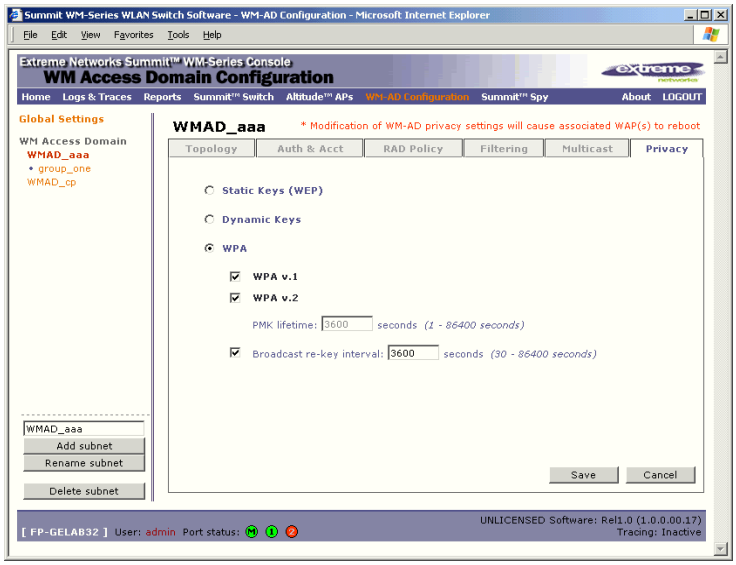
- a 128 bit key length, for the WPA2/802.11i implementation of AES
- four stages that make up one round. Each round is iterated 10 times. a per-packet key mixing function that shares a starting key between devices, and then changes their encryption key for every packet or after the specified re-key time interval.
- the Counter-Mode/CBC-MAC Protocol (CCMP), a new mode of operation for a block cipher that enables a single key to be used for both encryption and authentication. The two underlying modes employed in CCM include
  - Counter mode (CTR) that achieves data encryption
  - Cipher Block Chaining Message Authentication Code (CBC-MAC) to provide data integrity

The steps in the WPA authentication and encryption process are as follows:

1. The wireless device client associates with Altitude AP.
2. Altitude AP blocks the client's network access while the authentication process is carried out (the Summit WM-Series Switch sends the authentication request to the RADIUS authentication server).
3. The wireless client provides credentials that are forwarded by the Summit WM-Series Switch to the authentication server.
4. If the wireless device client is not authenticated, the wireless client stays blocked from network access.
5. If the wireless device client is authenticated, the Summit WM-Series Switch distributes encryption keys to the Altitude AP and the wireless client.
6. The wireless device client gains network access via the Altitude AP, sending and receiving encrypted data. The traffic is controlled with permissions and policy applied by the Summit WM-Series Switch.

Set up Wi-Fi Protected Access privacy (WPA) for an AAA WM-AD

1 To set up WPA privacy on the WM-AD, click on the WPA radio button.


Summit WM-Series WLAN Switch Software - WM-AD Configuration - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Extreme Networks Summit™ WM-Series Console
WM Access Domain Configuration
Home Logs & Traces Reports Summit™ Switch Altitude™ APs WM-AD Configuration Summit™ Spy About LOGOUT
Global Settings
WM Access Domain
WMAD_aaa
group_one
WMAD_cp
WMAD_aaa
* Modification of WM-AD privacy settings will cause associated WAP(s) to reboot
Topology Auth & Acct RAD Policy Filtering Multicast Privacy
Static Keys (WEP)
Dynamic Keys
WPA
WPA v.1
WPA v.2
PMK lifetime: 3600 seconds (1 - 86400 seconds)
Broadcast re-key interval: 3600 seconds (30 - 86400 seconds)
WMAD_aaa
Add subnet
Rename subnet
Delete subnet
Save
Cancel
[FP-GELAB32] User: admin Port status:
UNLICENSED Software: Rel1.0 (1.0.0.00.17)
Tracing: Inactive

2 To enable either **WPA v1** or **WPA v2**, or both, click the appropriate checkboxes on.

3 To enable re-keying after a time interval, click the **Broadcast re-key interval** checkbox on (the default is on). Type in the re-key time interval (the time after which the broadcast encryption key is changed automatically) in seconds.

If the box is unchecked, the Broadcast encryption key is never changed and the Altitude AP will always use the same broadcast key for Broadcast/Multicast transmissions. Note that this reduces the level of security for wireless communications.

4 To save the privacy parameters for the new WM-AD, click on the **Save** button.

A WM-AD with no authentication

You can choose to set up a WM-AD that will bypass all authentication mechanisms and run Summit WM-Series Switch Software with no authentication of a wireless device user.

On such a WM-AD, however, you can still control network access with filtering rules. See "The non-authenticated filter for Captive Portal" on page 87 for information on how to set up filtering rules that allow access only to specified IP addresses and ports.

Set up a WM-AD with no authentication

1 In the *WM Access Domain Configuration* screen, highlight the WM-AD name in the left-hand list and click on the **Topology** tab.

2 In the *Topology* screen, select **Network Assignment by SSID**. Follow the steps described above for a WM-AD for Captive Portal. Save the new WM-AD Topology by clicking on the **Save** button.

3 Click on the **Authentication** tab for this WM-AD. Click on the **Configure Captive Portal** button.

4 In the *Configure Captive Portal* subscreen, select the **No Captive Portal** radio button, for no authentication on this WM-AD, then click on the **Save** button.

5 In the *Filtering* screen, define a Non-Authenticated Filter that will control specific network access for any wireless device users on this WM-AD. These rules should be very restrictive. The final rule should be a "Deny All" rule. The Non-Authenticated Filter for a WM-AD with no authentication will not have a Captive Portal page for login.

A WM-AD for voice traffic

Voice data traffic on a wireless network

New developments are enabling the integration of internet telephony technology on wireless networks – Voice over Internet Protocol (VoIP) using 802.11 wireless local area networks (WLANs).

VoIP over 802.11 WLANs raises various issues including quality-of-service (QoS), call control, network capacity, and network architecture.

Wireless voice data requires a constant transmission rate and must be delivered within a time limit. This type of data is called *isochronous* data. This requirement for isochronous data is in contradiction to the concepts in the 802.11 standard that allow for data packets to wait their turn, to avoid data collisions. (Regular traffic on a wireless network is an *asynchronous* process in which data streams are broken up by random intervals.)

The solution is to add mechanisms to the network that give voice data traffic priority over all other traffic, and allow for continuous transmission of voice traffic.

Summit WM-Series Switch Software provides advanced Quality of Service (QoS) management, in order to provide better network traffic flow. Such techniques include:

- WMM (Wi-Fi Multimedia): enabled globally on the Altitude AP, for devices with WMM enabled., the standard provides multimedia enhancements that improve the user experience for audio, video, and voice applications. WMM is part of the 802.11e standard for QoS.
- IP ToS (Type of Service) or DSCP (Diffserv Codepoint): the ToS/DSCP field in the IP header of a frame is used to indicate the priority and Quality of Service for each frame. The IP TOS and/or DSCP is maintained within CTP (CAPWAP Tunneling Protocol) by copying the user IP QoS information to the CTP header — this is referred to as Adaptive QoS.

Quality of Service (QoS) management is also provided by:

- assigning high priority to a WM-AD
- static configuration of an SSID
- support for legacy devices that use SpectraLink Voice Protocol (SVP) for prioritizing voice traffic

Setting up a WM-AD for voice traffic

In order to set up a WM-AD for voice-over-internet traffic, a number of factors should be taken into account, on the enterprise network and in the Summit WM-Series Switch Software system.

On the enterprise network, the wireless telephone users will require access to:

- a private branch exchange (PBX), a private telephone system within an enterprise, with such features as voicemail.

- a Telephony Gateway, for access to an external standard telephone network, such as the wireless cellular network or the public switched telephone network (PSTN). The Telephony Gateway should be located on the same subnet as the Summit WM-Series Switch.

For large deployments, an SVP server is required on the enterprise network, if Spectralink devices are to be supported.

In Summit WM-Series Switch Software, configure the WM-AD for voice-over-internet traffic as follows:

1 In the *Topology* screen, set network assignment by **SSID**

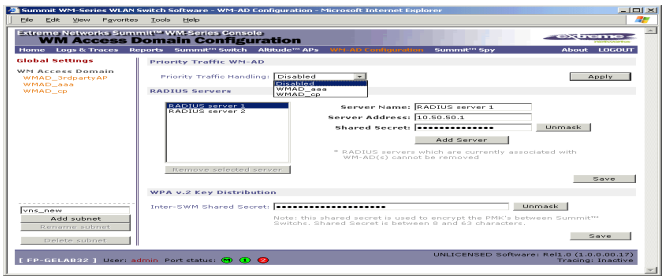
2 In the *Authentication* screen, set authentication to **No Captive Portal** (no authentication), since wireless telephone users do not have a user interface in which they can enter authentication identification

3 In the *Multicast* screen,
   - enable Multicast by clicking the checkbox on
   - define the multicast groups by IP address range, or select a predefined multicast group from the drop-down list (such as Spectralink-enabled devices using the SVP Protocol).

4 In the *Filtering* screen, define rules that allow access to the DNS server, to the Telephony Gateway, and then deny all other traffic

5 In the *Privacy* screen, set privacy to use 104-bit WEP key (recommended for greater security).

6 As the final step, in the *Global Settings* screen, from the **Priority Traffic Handling** drop-down list, select the WM-AD name to which this priority will apply:



Configure the Altitude AP radio for a voice traffic WM-AD

In the *Altitude AP Configuration* screen, make the following changes on the Altitude AP radio for this WM-AD, to support SVP requirements:

1 Set the 2.4 Ghz radio to support only B mode (G mode not supported).

2 Set the operational radio rate to **Best data rate**.

3 The save these modifications, click on the **Save** button.

7 Summit WM-Series Switch Configuration: Availability and Mobility

Availability

The Summit WM-Series Switch Software system provides a feature that maintains service availability in the event of a Summit WM-Series Switch outage.

The Availability feature links two Summit WM-Series Switches as a pair, so that they share information about their Altitude APs. If one Summit WM-Series Switch in a pair fails, then its Altitude APs are allowed to connect instead to the second Summit WM-Series Switch. The second Summit WM-Series Switch provides the wireless network and a pre-assigned WM-AD for the Altitude AP.

From the viewpoint of a Altitude AP, if its home Summit WM-Series Switch fails, the Altitude AP reboots and begins its discovery process. The Altitude AP will be directed to the appropriate second Summit WM-Series Switch of the pair.

NOTE

The Availability feature relies on SLP and a DHCP server that supports Option 78, as described earlier in the Altitude AP discovery and registration process. The Availability feature controls how the paired Summit WM-Series Switches register as services with SLP, in normal operations and in the event of an outage.

The wireless device users that were on the Altitude AP must log in again and become authenticated on the second Summit WM-Series Switch.

The Availability feature is set up in the Altitude AP Registration Mode screen.

Prepare for setting up the Availability feature

Before you begin, the following preparation should be done:

- Choose which Summit WM-Series Switch is the primary and which is the secondary.
- Determine the physical communication link for the TCP/IP connection between the two Summit WM-Series Switches (this is done over TCP port 13907), and ensure that the interfaces used for this connection are routable.
- Set up DHCP to support Option 78 for SLP, so that it points to the IP addresses of the physical interfaces on both Summit WM-Series Switches that the Altitude APs are connected to, or can reach after the Availability setup.

Now set up each Summit WM-Series Switch separately. One method is as follows:

1 In the *AP Registration* screen, set up each Summit WM-Series Switch in "Stand-alone Mode" and "Secure Mode" (allow only approved Altitude APs to connect).

2 In the *WM-AD Configuration*, *Topology* screen, define a WM-AD on each Summit WM-Series Switch with the same SSID (but different IP addresses).

3 On one Summit WM-Series Switch, allow all Altitude APs to associate with it. Then set the Registration Mode to "Allow only approved" so that no more Altitude APs can register.

4 On the other Summit WM-Series Switch that is to be paired, allow all Altitude APs to associate with it. Then set the Registration Mode to "Allow only approved" so that no more Altitude APs can register

5 In the *AP Registration* screen, now enable the two Summit WM-Series Switchs as a pair, as described below.

6 On each Summit WM-Series Switch, in the *Access Approval* screen, check the status of the Altitude APs. Each set of Altitude APs on the home Summit WM-Series Switch should appear as "local" while those on the other Summit WM-Series Switch should appear as "foreign".

A second method to set up the Summit WM-Series Switchs is as follows:

1 In the *AP Registration* screen, enable the two Summit WM-Series Switchs as a pair, as described below.

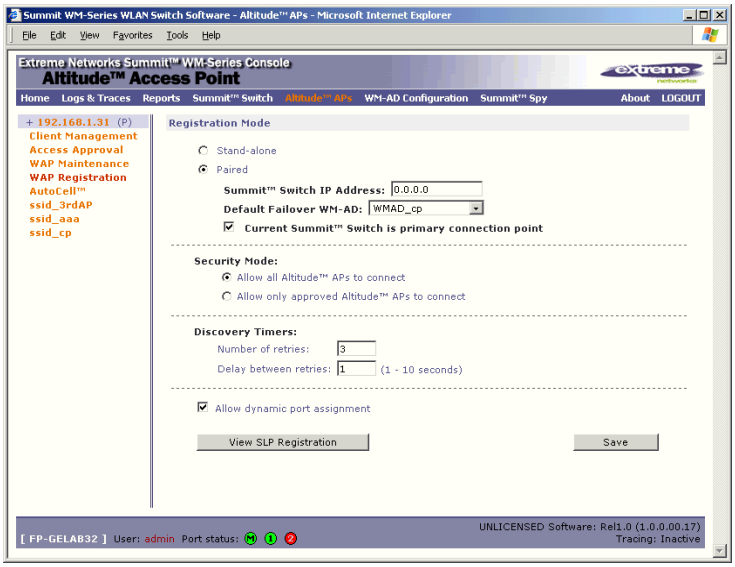
2 Add each Altitude AP manually to each Summit WM-Series Switch. (Select the **Altitude AP** tab. In the *Altitude AP Properties* screen, click on the **Add Altitude AP** button. The *Altitude AP Configuration* subscreen appears. Define the Altitude AP and click on the **Add Altitude AP** button. In the *Access Approval* screen, change the Altitude AP status from "Pending" to "Approved".)

WARNING!

If two Summit WM-Series Switches are paired and one has the "Allow All" option set for Altitude AP registration, all Altitude APs will register with that Summit WM-Series Switch.

Set up two Summit WM-Series Switches as a pair, for availability

1 On the Summit WM-Series Switch that is to be the primary, select **Altitude APs** tab. Click on **AP Registration**. The *Altitude AP Registration Mode* screen appears.



2 Click the **Paired** radio button.

3 Enter the **IP address** of the physical port of the secondary Summit WM-Series Switch. This IP must be on a routable subnet between the two Summit WM-Series Switches.

4 Select a **Default Failover WM-AD** on the other Summit WM-Series Switch from the drop-down list of WM-ADs (this list will be populated only after a WM-AD has been defined).

5 Since this Summit WM-Series Switch is to be the **primary connection point**, click the checkbox on.

6 Set the **Security Mode** to "Allow Approved" by clicking the radio button. [recommended after initial set up for paired Summit WM-Series Switches]

7 To save these settings, click on the **Save** button.

On the Summit WM-Series Switch that is to be the secondary one, repeat Steps 1 to 7, with these exceptions:

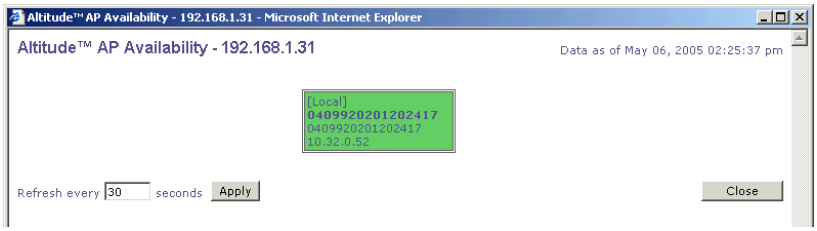
- In Step 3, enter the IP address of the Management port or physical port of the primary Summit WM-Series Switch.
- In Step 5, leave the primary connection point checkbox unchecked.

NOTE

When two Summit WM-Series Switches have been paired as described above, each Summit WM-Series Switch's registered Altitude APs will appear as "foreign" in the list of available Altitude APs when configuring a WM-AD topology.

View the Altitude AP Availability Display

When the Altitude AP Configuration: AP Registration Mode screen has been saved for the Summit WM-Series Switch in Paired Mode, the Altitude AP Availability display will show the status of both "local" and "foreign" Altitude APs for that Summit WM-Series Switch.

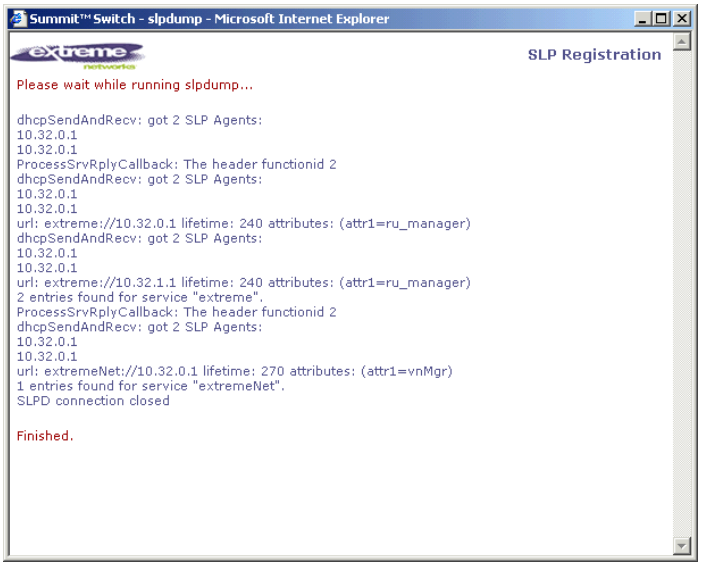


In normal operations, when Availability is enabled, the "local" Altitude APs are green, and the "foreign" Altitude APs are red. If the other Summit WM-Series Switch fails, and the "foreign" Altitude APs connect to the current Summit WM-Series Switch, the display will show all Altitude APs as green. If the Altitude APs are not attached they do not appear in the report.

View the SLP activity with the “slpdump tool”

1 In the *Altitude AP Registration Mode* screen, click on the **View SLP Registration** button. A popup screen displays the results of the diagnostic “slpdump tool”, to confirm SLP registration.

In normal operations, the primary Summit WM-Series Switch registers as an SLP service called “ac_manager” and directs the Altitude APs to the appropriate Summit WM-Series Switch of a pair. During an outage, if the remaining Summit WM-Series Switch is the secondary one, it will register as an SLP service “ru_manager”.



Events and actions during a Failover

If one of the Summit WM-Series Switches in a pair fails, the connection between the two Summit WM-Series Switches is lost. This triggers a “Failover mode” condition, and a critical message appears in the information log of the remaining Summit WM-Series Switch.

After the Altitude AP on the failed Summit WM-Series Switch loses its connection, it will attempt a reboot. Because of the pairing of the two Summit WM-Series Switches, the Altitude AP will then register with the other Summit WM-Series Switch.

NOTE

A Altitude AP connects first to a Summit WM-Series Switch registered as “ac_manager” and, if not found, then seeks an “ru_manager”. If the primary Summit WM-Series Switch fails, the secondary one registers as “ru_manager”. This enables the secondary Summit WM-Series Switch to be found by Altitude APs after they reboot.

When the Altitude APs connect to the second Summit WM-Series Switch, they will be assigned to the Failover WM-AD defined in setup in that Summit WM-Series Switch. The wireless device users will log in again and be authenticated on the second Summit WM-Series Switch.

When the failed Summit WM-Series Switch recovers, each Summit WM-Series Switch in the pair goes back to normal mode. They exchange information that includes the latest lists of registered Altitude APs. The administrator will release the Altitude APs on the second Summit WM-Series Switch, so that they may re-register with their home Summit WM-Series Switch.

To support the Availability feature during a "Failover" event, administrator will need to perform the following actions:

1 Monitor the critical messages for the "Failover mode" message, in the information log of the remaining Summit WM-Series Switch (in the *Reports and Displays* area).

2 After recovery, on the Summit WM-Series Switch that did not fail, select the "foreign" Altitude APs and click on the **Release** button (in the *Altitude AP Configuration - AP Maintenance* screen).

Mobility and the WM-AD Manager

The Summit WM-Series Switch Software system has a technique by which multiple Summit WM-Series Switches on a network can discover each other and exchange information about a client session. This enables a wireless device user to roam seamlessly between different Altitude APs on different Summit WM-Series Switches.

The solution introduces the concept of a "WM-AD Manager". This means that one Summit WM-Series Switch on the network must be designated as the "WM-AD Manager". All other Summit WM-Series Switchs are designated as "WM-AD Agents". To define whether the Summit WM-Series Switch is a Manager or an Agent, use the *WM-AD Manager* screen in the Summit WM-Series Switch Configuration area.

The wireless device will keep the IP address, WM-AD assignment and filtering rules that it received from the Summit WM-Series Switch that it first connected to - its "home" Summit WM-Series Switch. (This information is collected in the *Active Clients by WM-AD* display on the home Summit WM-Series Switch.) The WM-AD on each Summit WM-Series Switch must have the same SSID. If the WM-AD has static WEP, it is recommended that the same key be used.

NOTE

The "WM-AD Manager" concept relies on SLP and DHCP. Before you begin, you must ensure that the DHCP server on your network supports Option 78. These are also used during the Altitude AP discovery process, explained earlier in this Guide.

VW-AD Manager and VW-AD Agent: Background

The Summit WM-Series Switch that is the "WM-AD Manager":

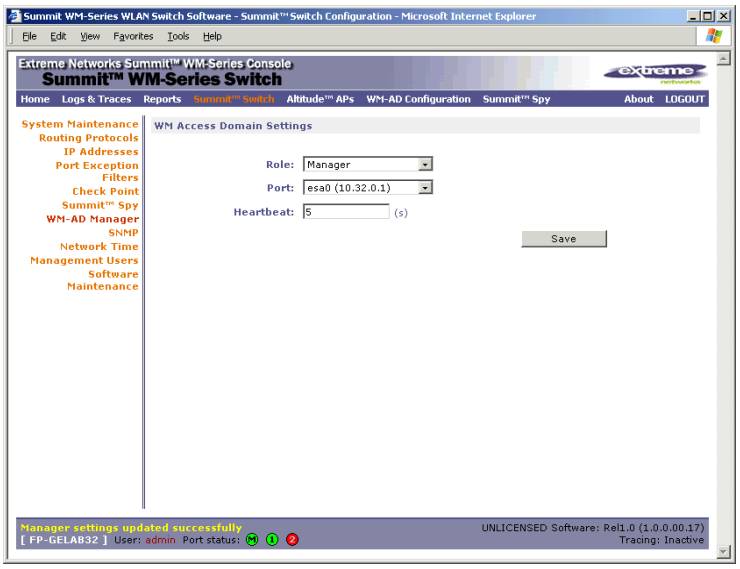
- uses SLP to register itself (as "ExtremeNet") with the SLP Directory Agent
- listens for connection attempts from "WM-AD Agents"
- if it receives a connection attempt from "WM-AD Agent", establishes connection and sends a message to the "WM-AD Agent" specifying the Heartbeat interval, and the WM-AD Manager's IP address
- sends regular Heartbeat messages (which contain wireless device session changes and Agent changes) to the WM-AD Agents and waits for an Update message back
- if it fails to receive an Update from the WM-AD Agent after three Heartbeat messages, sends a Disconnect message to the WM-AD Agent, removes all wireless device users associated with that WM-AD Agent Summit WM-Series Switch from its tables and closes down the connection.

The Summit WM-Series Switch that is a "WM-AD Agent":

- uses SLP to find the location of the WM-AD Manager
- attempts to establish a TCP/IP connection with the WM-AD Manager
- when it receives the connection-established message (see above), updates its tables, and sets up data tunnels to and between all Summit WM-Series Switchs it has been informed of
- after every Heartbeat massage received, uses the information to update its own tables and then sends an Update message to the WM-AD Manager, with updates on wireless device users and data tunnels it is managing.

Set up a Summit WM-Series Switch as a WM-AD Manager

1 In the *Summit WM-Series Switch Configuration* screen, click on the **WM-AD Manager** option. The *WM Access Domain Settings* screen appears.



2 From the **Role** drop-down list, select **WM-AD Manager** (other options: None, Agent).

3 From the drop-down list, select the **Port** on the Summit WM-Series Switch to be used by the WM-AD Manager process. Ensure that the port selected is routable on the network.

4 In the **Heartbeat** field, type in the time interval at which the WM-AD Manager sends a Heartbeat message to a WM-AD Agent. The default is 5 seconds.

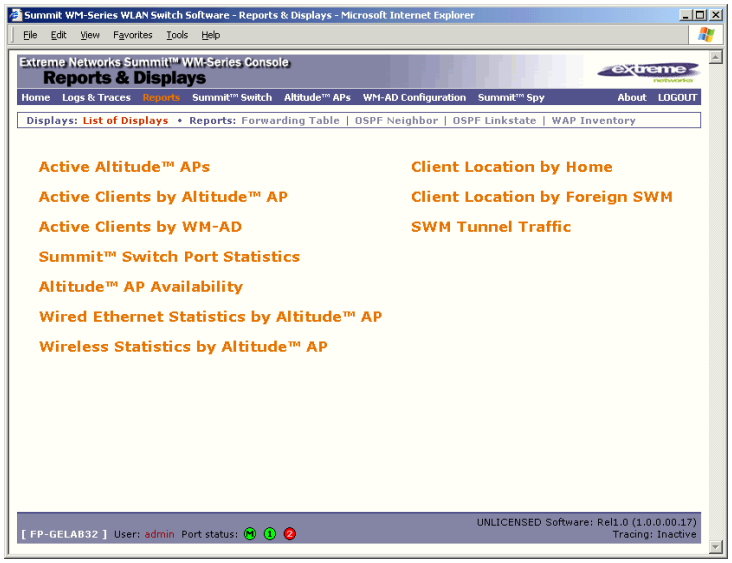
5 To save these settings, click on the **Save** button.

If you set up one Summit WM-Series Switch on the network as a "WM-AD Manager", then all other Summit WM-Series Switchs must be set up as "WM-AD Agents". In the *WM-AD Manager* screen, in the **Role** drop-down list, select **Agent**. The **Heartbeat** value for a "WM-AD Agent" is how long to wait for a connection establishment response before trying again.

View additional displays when WM-AD Manager is enabled

On a Summit WM-Series Switch has been configured as a WM-AD Manager, three additional displays appear as options in the *List of Displays* screen:

- *Client Location by Home*: shows the active wireless clients, listed by their "Home" Summit WM-Series Switch
- *Client Location by Foreign SWM*: shows the active wireless clients, listed by the foreign Summit WM-Series Switch they are active on
- *SWM Tunnel Traffic*: shows the status of the tunnels between the Summit WM-Series Switches.


Summit WM-Series WLAN Switch Software - Reports & Displays - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Extreme Networks Summit™ WM-Series Console
Reports & Displays
Home Logs & Traces Reports Summit™ Switch Altitude™ APs WM-AD Configuration Summit™ Spy About LOGOUT
Displays: List of Displays • Reports: Forwarding Table | OSPF Neighbor | OSPF Linkstate | WAP Inventory
Active Altitude™ APs
Active Clients by Altitude™ AP
Active Clients by WM-AD
Summit™ Switch Port Statistics
Altitude™ AP Availability
Wired Ethernet Statistics by Altitude™ AP
Wireless Statistics by Altitude™ AP
Client Location by Home
Client Location by Foreign SWM
SWM Tunnel Traffic
[FP-GELAB32] User: admin Port status:
UNLICENSED Software: Rel1.0 (1.0.0.00.17)
Tracing: Inactive

To view the status of the tunnels between the Summit WM-Series Switches, click on the *SWM Tunnel Traffic* option. This screen displays the Summit WM-Series Switches known to the WM-AD Manager. If a tunnel is active, a green band is displayed between Summit WM-Series Switches. A red band indicates that there is no traffic on the tunnel. If the Summit WM-Series Switches are not displayed, the tunnel is inactive.

The *Active Clients by WM-AD* display also collects information on the WM-AD Manager Summit WM-Series Switches of for all Altitude APs, and for the wireless devices that travel, if they are on the same SSID.

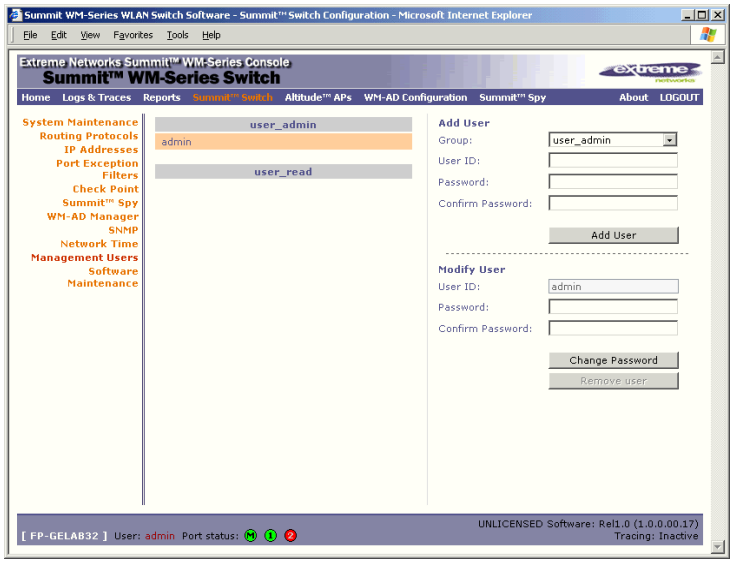
8 Summit WM-Series Switch: configuring other functions

Management users

In this screen you define the login usernames that have access to the GUI, either for Summit WM-Series Switch Software Administrators with “read/write” privileges, or users with “read only” privileges. For each user added, you can also define and modify a User ID and Password.

Designate Summit WM-Series Switch management users

1 Click on the **Summit Switch** tab. Click on the **Management Users** option. The *Management Users* screen appears.



The **user_Admin** list displays “Admin” users who have read/write privileges. The **user_read** list is for users who have “read only” privileges.

2 To add a user, select from the pull-down list whether this is an Admin or a "read only" user. Then in the entry field, type in the User ID. A User ID can only be used once, in only one category. Key in, and confirm, the password for this user. The $ character is not permitted.

3 Click on the **Add User** button.

4 To modify a user’s password, click on the name to select it, key in and confirm the new password. Then click on the **Change password** button.

5 To remove a user, click on the name to select it, then click on the **Remove user** button.

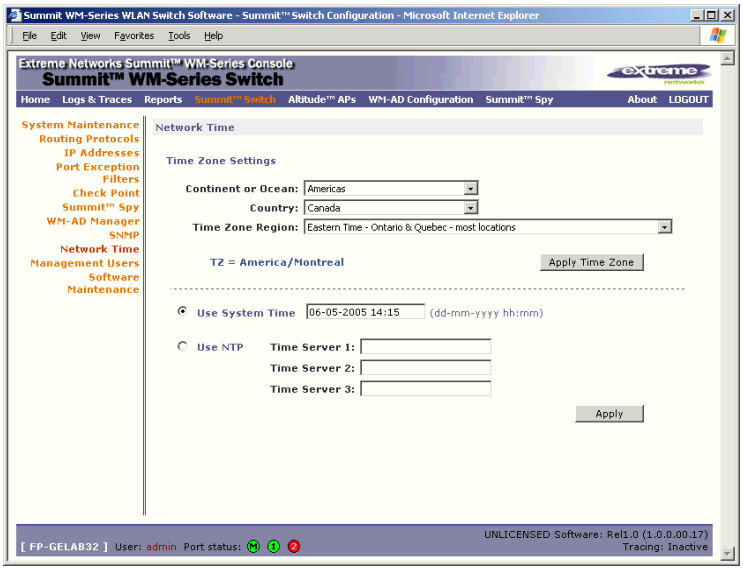
Network time

Use the Network Time screen to synchronize the elements on the network to a universal clock. This ensures accuracy in usage logs. Network time is synchronized in one of two ways:

- using system time
- using Network Time Protocol (NTP), an Internet standard protocol that synchronizes client workstation clocks.

Set Network Time parameters

1 Click on the **Summit Switch** tab. Click on the **Network Time** option. The *Network Time* screen appears.


Summit WM-Series WLAN Switch Software - Summit™ Switch Configuration - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Extreme Networks Summit™ WM-Series Console
Summit™ WM-Series Switch
Home Logs & Traces Reports Summit™ Switch Altitude™ APs WM-AD Configuration Summit™ Spy About LOGOUT
System Maintenance
Routing Protocols
IP Addresses
Port Exception Filters
Check Point
Summit™ Spy
WM-AD Manager
SNMP
Network Time
Management Users
Software Maintenance
Network Time
Time Zone Settings
Continent or Ocean: Americas
Country: Canada
Time Zone Region: Eastern Time - Ontario & Quebec - most locations
TZ = America/Montreal
Apply Time Zone
Use System Time 06-05-2005 14:15 (dd-mm-yyyy hh:mm)
Use NTP Time Server 1:
Time Server 2:
Time Server 3:
Apply
[FP-GELAB32] User: admin Port status:
UNLICENSED Software: Rel1.0 (1.0.0.00.17)
Tracing: Inactive

2 From the drop-down list, select the **Continent** or **Ocean**, the large-scale geographic grouping.

3 From the drop-down list, select the **Country**, within the previous group (the contents of the list will change based on the selection in the previous field).

4 From the drop-down list, select the **Time Zone Region** for the country selected.

5 To apply these time zone settings, click on the **Apply Time Zone** button.

6 To use **System Time**, click on its radio button. Type in the time setting.

7 To use Network Time Protocol, click on the **NTP** radio button. Then fill in the location (IP address or FQDN) of up to three standard NTP Time Servers.

8 To apply these settings, click on the **Apply** button

Check Point event logging

The Summit WM-Series Switch has the capability to forward specified event messages to an ELA server using the OPSEC ELA protocol - Event Logging API (Application Program Interface). On the ELA server (such as Check Point Management Console), the event messages are tracked and analyzed, so that suspicious messages can be forwarded to a firewall application (such as Check Point Firewall-1) that can take corrective action.

Check Point created the OPSEC (Open Platform for Security) alliance program for security application and appliance vendors to enable an open industry-wide framework for interoperability.

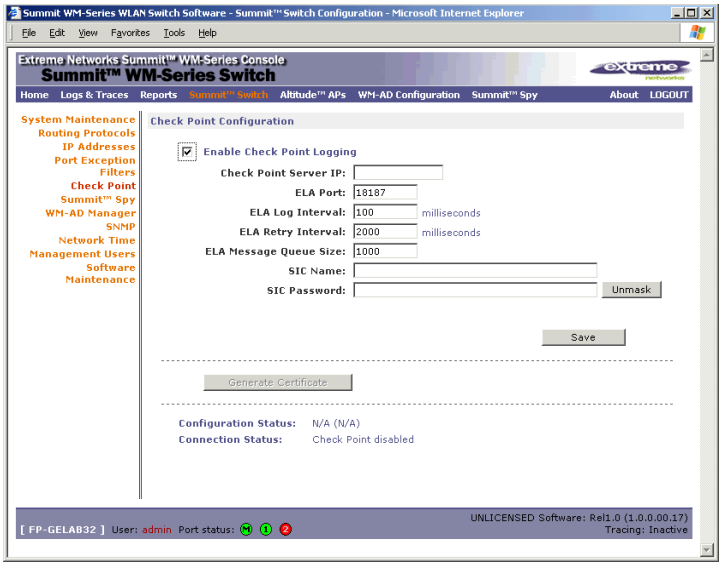
When ELA is enabled on the Summit WM-Series Switch, the Summit WM-Series Switch forwards the specified event messages from its internal event server to the designated ELA Management Station on the enterprise network.

NOTE

Before you set up the Summit WM-Series Switch, you must first create OPSEC objects for Summit WM-Series Switch in the Check Point management software. The name and password you define there must also be entered into the Summit WM-Series Switch Check Point configuration screen.

Enable and configure Check Point

1 Click on the **Summit Switch** tab. Click on the **Check Point** option. The *Check Point Configuration* screen appears.



2 To enable **Check Point Logging**, click the checkbox on.

3 Key in values in the following fields, or accept the defaults:

Check Point Server IP:	Type in the Check Point fw-1 IP address, the IP address of the ELA Management Station.
ELA Port:	Default port is 18187. Modify if desired.
ELA Log Interval:	Type in the amount of time (in milliseconds) you want the system to wait before attempting to log, once there is a connection between Summit WM-Series Switch and the Check Point gateway.
ELA Retrial Interval:	Type in the amount of time (in milliseconds) you want the system to wait before attempting a reconnection between Summit WM-Series Switch and the Check Point gateway.
ELA Message Queue size:	The number of messages the log queue will hold if Summit WM-Series Switch and the Check Point gateway become disconnected. The default value is 1000 log entries.
SIC Name:	Type in Secure Internal Communication (SIC) Name, your security-based ID. **Note:** Copy in this field the information displayed in the DN field in Secure Internal Communication (SIC) area of Check Point "Application Properties" screen. The DN (Distinguished Name) field displays a reminder of information you will need
SIC Password:	Type in your Secure Internal Communication (SIC) password. Use the Unmask button to display the password. **Note:** Copy in this field the Activation Key defined in OPSEC setup as the Certificate password.

4 To save these parameters, click on the Save button.

5 To create the certificate that is sent to the ELA Management Station, click on the Generate Certificate button.

6 If the certificate worked and the connection with the ELA Management Station is made, the Connection Status area displays a message "OPSEC Connection OK". If there is an error in generating the certificate or establishing the connection, the message "OPSEC Connection Error" appears.

The events for the ELA Management Station are grouped under Extreme Network and are mapped to two types: "info" and "alerts". The alerts include:

- Altitude AP registration and/or authentication failed.
- Authentication User Request unsuccessful.
- RADIUS server rejected login (Access Rejected).
- An unknown AP has attempted to connect. AP authentication failure.
- A connection request failed to authenticate with the CM messaging server. (This may indicate port-scanning the Summit WM-Series Switch, or a backdoor access attempt.)
- Unauthorized client attempting to connect.

Setting up SNMP

The Summit WM-Series Switch Software system supports Simple Network Management Protocol (SNMP), Version 1 and 2c, for retrieving Summit WM-Series Switch statistics and configuration information.

Simple Network Management Protocol, a set of protocols for managing complex networks, sends messages, called protocol data units (PDUs), to different parts of a network. Devices on the network that are SNMP-compliant, called agents, store data about themselves in Management Information Bases (MIBs) and return this data to the SNMP requesters.

MIB support

The Summit WM-Series Switch Software system accepts SNMP "Get" commands and generates "Trap" messages. Support is provided for the retrieval information from the router MIB-II (SNMP_GET) as well as SNMP traps, and for the retrieval of wireless information from the 802.11 MIB.

For **MIB-II** (RFC1213), the following groups for the router characteristics of the Summit WM-Series Switch are supported:

- System Group
- Interfaces Group
- Address Translation Group
- IP Group
- ICMP Group
- TCP Group
- UDP Group

NOTE

Because of limitations in data captured in the control / data planes, MIB II compliance is incomplete. For example, esa/IXP ports can only provide the interface statistics.

For the **802.11 MIB** (IEEE 802.11 standard), the following are supported:

- IANAif Type-MIB
- IF-MIB
- INET-ADDRESS-MIB
- IP-FORWARD-MIB
- SNMPv2-MIB
- SNMPv2-SMI
- SNMPv2-TC

The Extreme **Enterprise MIB** includes:

- EXTREME-BM-MIB
- EXTREME-PRODUCTS-MIB

- EXTREME-SMI
- EXTREME-DOT11-EXTNS-MIB
- EXTREME-BEACON-CELL-MIB
- EXTREME-BRANCH-OFFICE-MIB

The MIB is provided for compilation into an external NMS. No support has been provided for automatic device discovery by an external NMS.

The Summit WM-Series Switch is the only point of SNMP access for the entire system. In effect, the Summit WM-Series Switch will proxy sets and gets and alarms from the associated Altitude APs.

Enabling SNMP on the Summit WM-Series Switch

If your enterprise network uses SNMP, you can enable SNMP on the Summit WM-Series Switch and define where the Summit WM-Series Switch should send the SNMP messages.

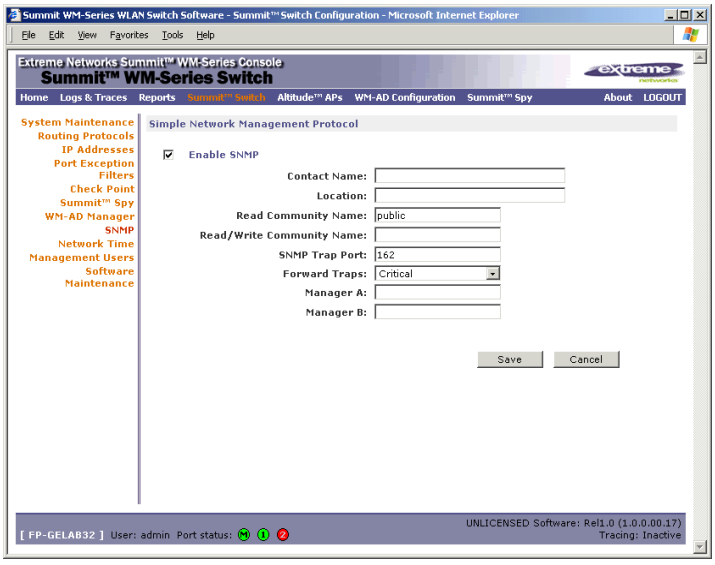
To enable SNMP traps, ensure that the following three fields are defined in the *Simple Network Management Protocol* screen:

- SNMP port
- Read Community
- Manager A and/or Manager B

The list of SNMP traps supported can be found in the Extreme MIB.

Setting SNMP Parameters

1 Click on the **Summit WM-Series Switch** tab. Click on the **SNMP** option. The *Simple Network Management Protocol* screen appears.



2 Key in:

Contact Name:	The name of SNMP administrator.
Location:	Location of the SNMP administration machine (descriptive).
Read Community Name:	Key in the password for Read activity.
Read/Write Community Name:	Key in the password for Read/Write activity. (Write ability is not supported.)
SNMP Port:	Key in the destination port for SNMP traps. The industry standard is 162. [If left blank, no traps are generated.]
Forward Traps:	From the drop-down list, select the severity level of the traps to be forwarded: Informational, Minor, Major, Critical.
Manager A:	The IP address of the specific machine on the network where the SNMP traps are monitored.
Manager B:	The IP address of a second machine on the network where the SNMP traps are monitored, if Manager A is not available.

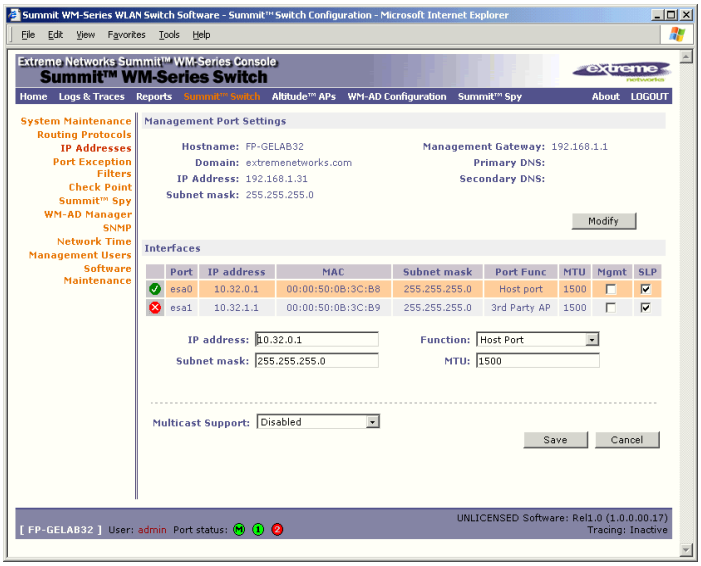
9 Setting up third-party access points

Your enterprise's WLAN may have existing third-party access points that you would like to integrate into the Summit WM-Series Switch Software WLAN solution. You can set up the Summit WM-Series Switch to handle wireless device traffic from third-party access points, providing the same policy and network access control.

Set up third-party access points on the Summit WM-Series Switch

1 Define one data port as a "3rd-party AP" port:

In the *Summit WM-Series Switch Configuration* screen, click on the **IP Address** option. The *Management Port Settings and Interfaces* screen appears. Highlight the appropriate port, and in the **Function** field, select "3rd-party AP" from the drop-down list. Make sure that Management Traffic and SLP are disabled for this port.



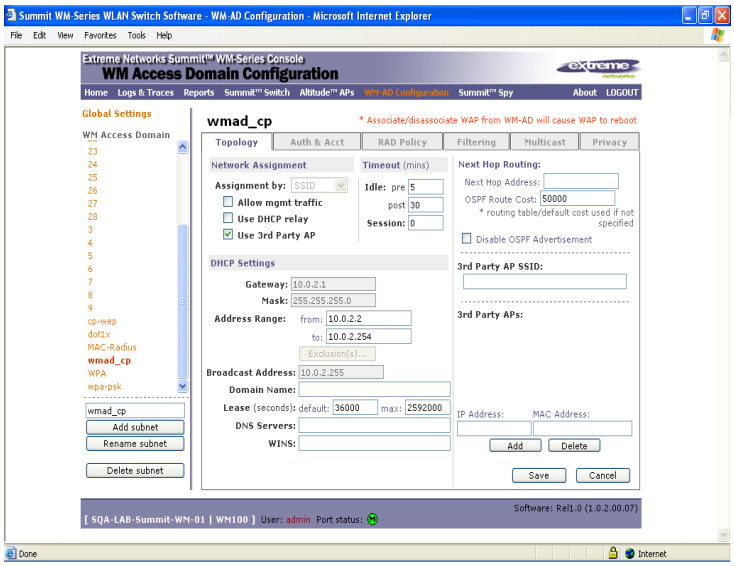
2 Connect the third-party access point to this port, via a switch.

3 Define a static route to the access point:

In the *Summit WM-Series Switch Configuration* screen, click on the **Routing Protocols** option. Then click the **Static Routes** tab. The *Static Routes* screen appears. Define a static route to the access point (see "Setting up static routes" on page 35).

4 Set up a WM-AD for the "3rd-party AP" port:

In the *WM Access Domain Configuration* screen, add a new WM-AD. Then highlight the WM-AD name in the left-hand list and click on the **Topology** tab.



In the *Topology* screen, select **Assignment by SSID**.

Click on the **Use 3rd Party AP** checkbox to select it.

Fill in the **IP Address** and **MAC Address** entry fields that appear on the right (the addresses of the third party access points, and click on the **Add** button. They will appear in the list of access points known to the Summit WM-Series Switch.

Follow the remaining steps described in the setting up a WM-AD for Captive Portal earlier in this Guide.

5 Set up Authentication by Captive Portal for the "3rd-party AP" WM-AD:

Click on the **Authentication** tab. In the *Authentication* configuration screen, click the **Captive Portal** radio button. In the *Captive Portal* portion of the screen, define the RADIUS Attributes and the Filter IDs to match those in RADIUS.

NOTE

Alternatively, for third-party APs, you can define network assignment by AAA, and authentication by 802.1x. The RADIUS requests from the third-party access point will flow through the Summit WM-Series Switch.

6 Set up filtering rules for the third-party APs:

Because the third-party APs are mapped to a physical port, you must define the Exception filters on the physical port, using the Port Exception Filters screen. See "Port-based exception filters: user defined" on page 39.

Define filtering rules that allow access to other services and protocols on the network such as HTTP, FTP, Telnet, SNMP.

In addition, modify the following functions on the third-party access point:

- Disable the access point's DHCP server, so that the IP address assignment for any wireless device on the AP is from the DHCP server at the Summit WM-Series Switch with WM-AD information.

- Disable the third-party access point's layer-3 IP routing capability and set the access point to work as a layer-2 bridge.

Here are the differences between third-party access points and Altitude APs on the Summit WM-Series Switch Software system:

- A third-party access point exchanges data with the Summit WM-Series Switch's data port using standard IP over ethernet protocol. The third-party access points do not support the tunnelling protocol for encapsulation.
- For third-party access points, the WM-AD is mapped to the physical data port and this is the default gateway for mobile units supported by the third-party access points.
- A Summit WM-Series Switch cannot directly control or manage the configuration of a third-party access point.
- Third-party access points are required to broadcast an SSID unique to their segment. This SSID cannot be used by any other WM-AD.
- Roaming from third-party access points to Altitude APs is not supported.

10 Summit Spy: detecting rogue access points

Overview

The Summit WM-Series Switch Software system includes a mechanism that assists in the detection of rogue access points. The function is called the Summit Spy.

The Summit Spy feature has three components:

- a radio frequency (RF) scanning task that runs on the Altitude AP. The Altitude AP itself functions as a scan device. Its scan function alternates with providing its regular service the wireless devices on the network. You set up the scan parameters in the Summit Spy user interface.
- an application called the RF Data Collector (RFDC) on the Summit WM-Series Switch that receives and manages the RF scan messages sent by the Altitude AP. The scan data includes lists of all connected Altitude APs, third Party APs and other friendly APs and the RF scan information that has been collected from the Altitude APs.
- an Analysis Engine on the Summit WM-Series Switch that processes the scan data from the RFDC through algorithms that make decisions about whether a detected access point is a rogue access point.

NOTE

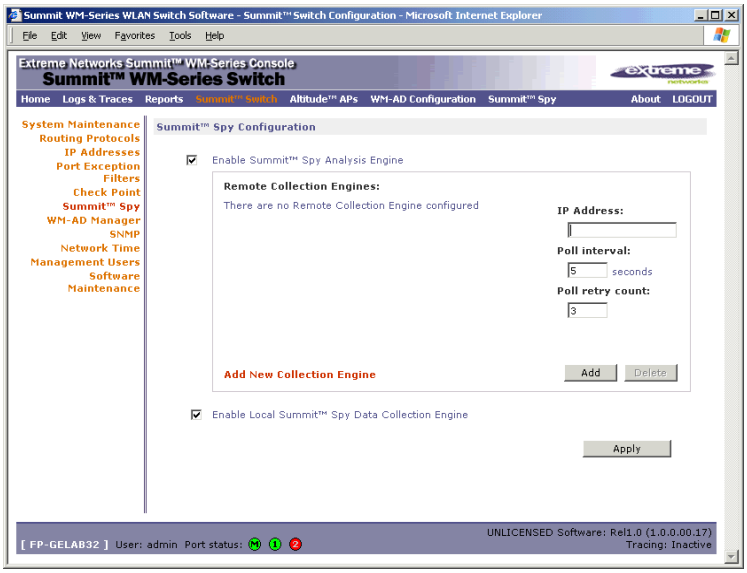
In a network with more than one Summit WM-Series Switch, the analysis engine should be active on only one Summit WM-Series Switch that communicates with the RFDC applications running on itself and on the other Summit WM-Series Switchs on the network. Ensure that these are all routable.

To use the Summit Spy, you must first enable it in the *Summit WM-Series Switch Configuration* area of the user interface.

Enabling the Analysis and RFDC Engines

Enable and configure the Summit Spy Analysis Engine

1 In the *Summit WM-Series Switch Configuration* screen, click on the **Summit Spy** option. The *Summit Spy Configuration* screen appears.



2 To enable the Summit Spy Analysis Engine, click the checkbox on.

Define the Summit Spy RF Data Collector Engines

3 To enable the **Summit Spy Data Collection Engine** on this Summit WM-Series Switch click the checkbox on.

4 Identify the remote RF Data Collector Engines that the Analysis Engine will poll for data: In the **Collection Engine IPs** entry field, key in the IP address of the Summit WM-Series Switch on which the remote RFDC resides. (For this Summit WM-Series Switch, the local IP address is displayed by default.)

5 For each data collection engine, enter:

- In the **Poll interval** field (the interval that the Analysis Engine polls the RF Data Collector for data), key in the time in seconds. Default is 30 seconds.
- In the **Poll retry count** field, key in the number of times the Analysis Engine will attempt to poll the RF Data Collector for data before it stops sending requests. Default is 2 attempts.

6 Click on the **Add** button. The IP address of the Data Collection Engine, with its Poll Interval and Poll Retry parameters, appears in the list.

NOTE

For each remote RF Data Collection Engine you define here, you must also:
> enable it (click the checkbox on) in the same screen on the remote Summit WM-Series Switch
> ensure that static routes are defined between the Summit WM-Series Switchs.

7 To clear the entry fields and add a new Collection Engine, click on the **Add Collection Engine** option. Repeat steps 4 to 6 above.

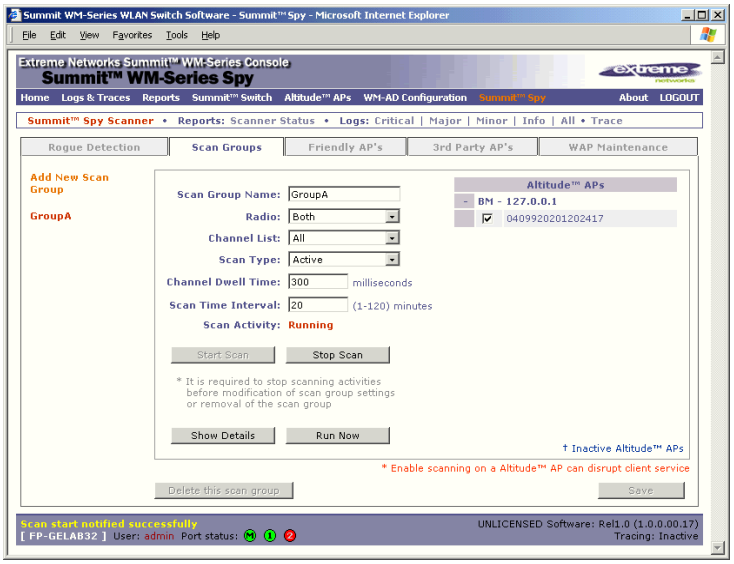
8 To save these settings, click on the **Apply** button.

Summit Spy: running scans

After enabling the Summit Spy engines (as described above), click the Summit Spy menu item in the main menu, or the **Summit Spy** tab in any screen. The *Summit Spy Scanner* screen appears, with five tabs.

Set up and run the Summit Spy scan task mechanism:

1 To set up the parameters of the scan task mechanism, click on the **Scan Groups** tab. The *Scan Groups* screen appears.


Summit WM-Series WLAN Switch Software - Summit™ Spy - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Extreme Networks Summit™ WM-Series Console
Summit™ WM-Series Spy
Home Logs & Traces Reports Summit™ Switch Altitude™ APs WM-AD Configuration Summit™ Spy About LOGOUT
Summit™ Spy Scanner • Reports: Scanner Status • Logs: Critical | Major | Minor | Info | All • Trace
Rogue Detection Scan Groups Friendly AP's 3rd Party AP's WAP Maintenance
Add New Scan Group
GroupA
Scan Group Name: GroupA
Radio: Both
Channel List: All
Scan Type: Active
Channel Dwell Time: 300 milliseconds
Scan Time Interval: 20 (1-120) minutes
Scan Activity: Running
Start Scan Stop Scan
* It is required to stop scanning activities before modification of scan group settings or removal of the scan group
Show Details Run Now
Altitude™ APs
BM - 127.0.0.1
0409920201202417
† Inactive Altitude™ APs
* Enable scanning on a Altitude™ AP can disrupt client service
Delete this scan group
Save
Scan start notified successfully
[FP-GELAB32] User: admin Port status:
UNLICENSED Software: Rel1.0 (1.0.0.00.17)
Tracing: Inactive

2 In the **Scan Group Name** entry field, key in a name for this Scan Group.

3 In the **Altitude APs** area, clicking the checkbox on to select the Altitude AP (or Altitude APs) that will be included in this Scan Group and will perform the scan function.

A Altitude AP can participate in only one Scan Group at a time. It is recommended that the Scan Groups represent geographical groupings of Altitude APs.

4 In the **Radio** field, from the drop-down list select which radios on the Altitude AP are to perform the scan function: **Both**, **A only**, **B/G only**.

5 In the **Channel List** field, from the drop-down list select the radio channels to scan on: **All** or **Current**.

6 In the **Scan Type** field, from the drop-down list select either **Active** or **Passive**.

- Active: the Altitude AP sends out ProbeRequests and waits for ProbeResponse messages from any access points.
- Passive: the Altitude AP listens for 802.11 beacons

7 In the **Channel Dwell Time** field, key in the time in milliseconds that the scanner waits for a response (either for 802.11 beacons in passive scanning, or ProbeResponse in active scanning).

8 In the **Scan Time Interval** field, key in the time in minutes {1 to 120}, to define the frequency at which a Altitude AP within the Scan Group will initiate a scan of the RF space.

9 To start a scan, using the periodic scanning parameters defined above, click on the **Start Scan** button

10 To initiate an immediate scan that will run once, click on the **Run Now** button.

A scan will not run on an inactive AP, even though it appears as part of the Scan Group. It it become active, it will be sent a scan request during the next periodic scan.

11 To stop the scan, click on the **Stop Scan** button.

NOTE

You must stop the scan before modifying any parameters of the Scan Group, or before adding or removing a Altitude AP from a Scan Group.

12 The **Scan Activity** field displays the current state of the scan engine.

13 To view a popup report showing the timeline of scan activity and results, click on the **Show Details** button.

The Analysis Engine

The Analysis Engine relies on a database of known devices on the Summit WM-Series Switch Software system as follows:

- Altitude APs registered with any Summit WM-Series Switch that has its RF Data Collector enabled and has been associated with the Analysis Engine on this Summit WM-Series Switch.
- Third-Party Access Points that have been defined and assigned to a WM-AD (as described earlier in this Guide).
- Friendly APs, a list created in the Summit Spy user interface as potential rogue access points are designated by the administrator as “Friendly”.
- Wireless devices registered with any Summit WM-Series Switch that has its RF Data Collector enabled and has been associated with the Analysis Engine on this Summit WM-Series Switch.

The Analysis Engine compares the data from the RF Data Collector with the above database of known devices.

The Analysis Engine looks for access points with seven conditions:

- unknown MAC address and unknown SSID (critical alarm)
- unknown MAC, with a valid SSID - a known SSID is being broadcast by the unknown access point (critical alarm)
- known MAC, with an unknown SSID - a rogue may be spoofing a MAC address (critical alarm)
- inactive Altitude AP with valid SSID (critical alarm)
- inactive Altitude AP with unknown SSID (critical alarm)

- known Altitude AP with an unknown SSID (major alarm)
- in ad-hoc mode (major alarm)

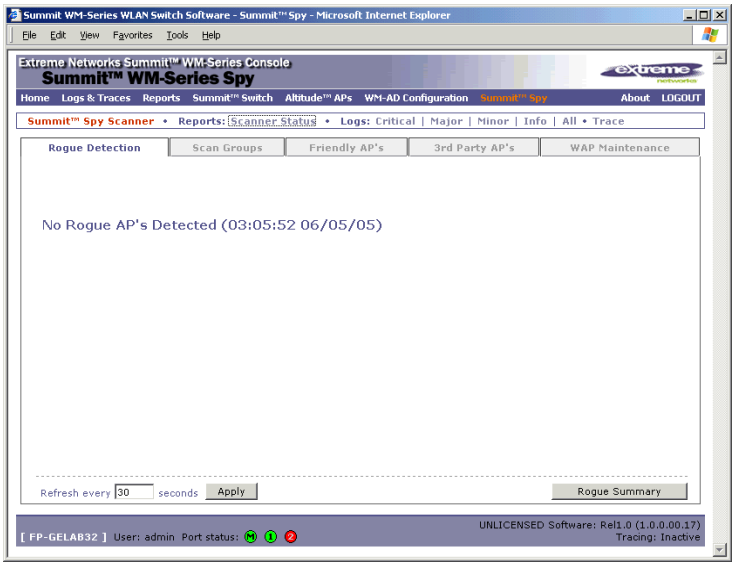
NOTE

In the current release, there is no capability to initiate a DoS attack on the detected rogue access point. Containment of a detected rogue will require an inspection of the geographical location of its Scan Group area (where its RF activity has been found).

View the Summit Spy scan results and build list of friendly APs

1 Click on the **Summit Spy** tab in any screen Then click on the **Rogue Detection** tab. The *Rogue Detection* screen appears displaying all access points and Altitude APs that were found in the scan but are not in the database of known devices (as defined above).

2 To modify the rate that this information is refreshed, key in a time in seconds and click on the **Apply** button.

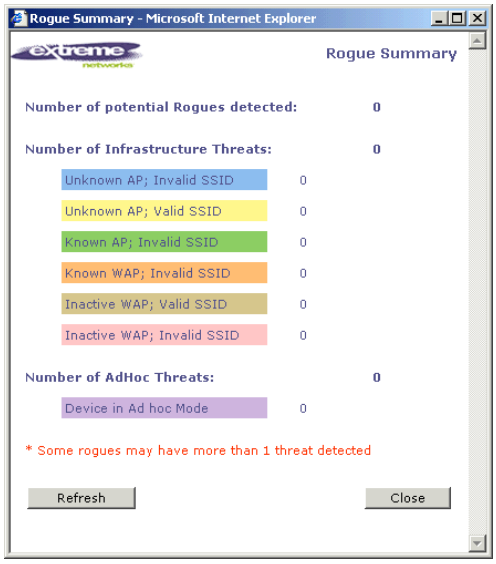

Summit WM-Series WLAN Switch Software - Summit™ Spy - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Extreme Networks Summit™ WM-Series Console
Summit™ WM-Series Spy
Home Logs & Traces Reports Summit™ Switch Altitude™ APs WM-AD Configuration Summit™ Spy About LOGOUT
Summit™ Spy Scanner • Reports: Scanner Status • Logs: Critical | Major | Minor | Info | All • Trace
Rogue Detection
Scan Groups
Friendly AP's
3rd Party AP's
WAP Maintenance
No Rogue AP's Detected (03:05:52 06/05/05)
Refresh every 30 seconds
Apply
Rogue Summary
[FP-GELAB32] User: admin Port status:
UNLICENSED Software: Rel1.0 (1.0.0.00.17)
Tracing: Inactive

3 To remove an access point from this list, click on the **Delete** button.

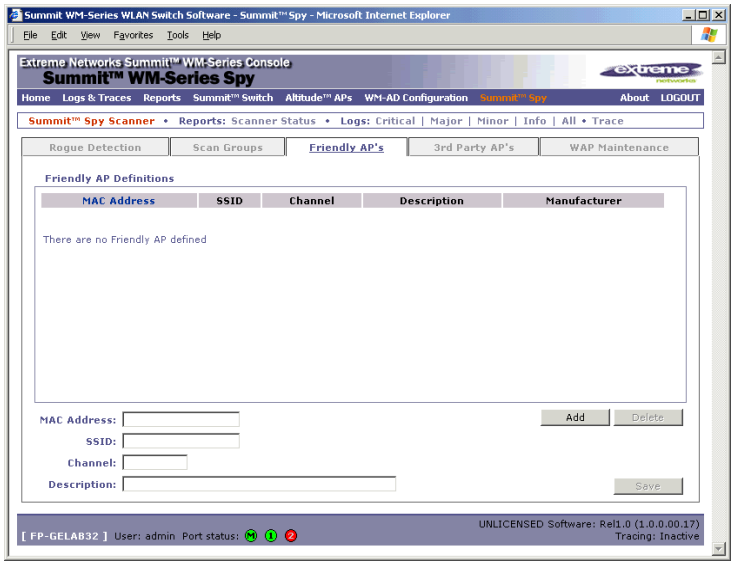
4 To add an access point or Altitude AP to the *Friendly APs* list, click on the **Add to Friendly List** button. The access point item will be removed from this list and will appear in the *Friendly APs* list.

A third-party access point will always appear first as a Rogue AP. Add it to the Friendly AP list as noted above.

5 Click the **Rogue Summary** button to view the *Rogue Summary* popup report.


Rogue Summary - Microsoft Internet Explorer
Rogue Summary
Number of potential Rogues detected: 0
Number of Infrastructure Threats: 0
Unknown AP; Invalid SSID 0
Unknown AP; Valid SSID 0
Known AP; Invalid SSID 0
Known WAP; Invalid SSID 0
Inactive WAP; Valid SSID 0
Inactive WAP; Invalid SSID 0
Number of AdHoc Threats: 0
Device in Ad hoc Mode 0
* Some rogues may have more than 1 threat detected
Refresh
Close

6 To view the Friendly list, click on the **Friendly APs** tab. The *Friendly AP Definitions* screen appears.


Summit WM-Series WLAN Switch Software - Summit™ Spy - Microsoft Internet Explorer
Extreme Networks Summit™ WM-Series Console
Summit™ WM-Series Spy
Home Logs & Traces Reports Summit™ Switch Altitude™ APs WM-AD Configuration Summit™ Spy About LOGOUT
Summit™ Spy Scanner • Reports: Scanner Status • Logs: Critical | Major | Minor | Info | All • Trace
Rogue Detection Scan Groups Friendly AP's 3rd Party AP's WAP Maintenance
Friendly AP Definitions
MAC Address SSID Channel Description Manufacturer
There are no Friendly AP defined
MAC Address:
SSID:
Channel:
Description:
Add Delete Save
[FP-GELAB32] User: admin Port status:
UNLICENSED Software: Rel1.0 (1.0.0.00.17)
Tracing: Inactive

7 To add friendly access points manually to the *Friendly AP Definitions* list, key in the **MAC Address**, **SSID**, **Channel**, and a text description of the access point. Click on the **Add** button. The new access point appears in the list above.

8 To delete an access point from the list, highlight it and click on the **Delete** button.

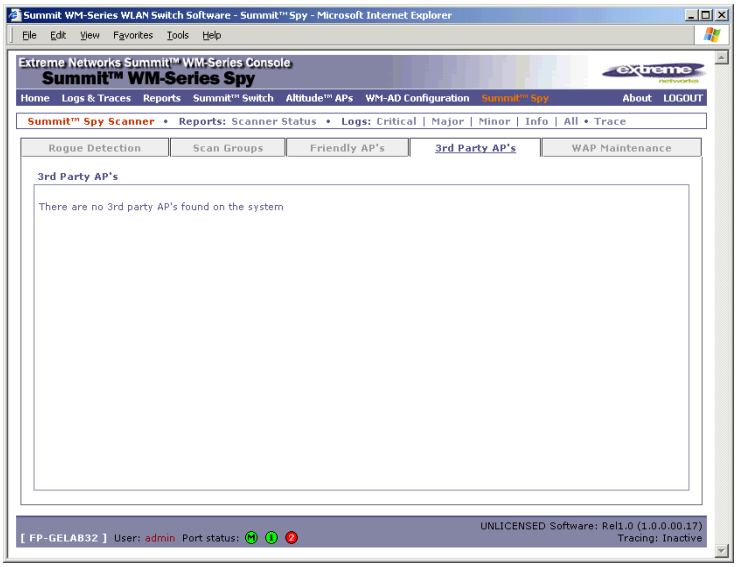
9 To modify an access point in the list, highlight it and make the appropriate changes in the entry fields. Click on the **Save** button.

NOTE

To avoid the Summit Spy's database becoming too large, it is recommended that you either delete Rogue APs or add them to Friendly AP list, rather than leaving them in the Rogue list.

View the Summit Spy list of Third-Party APs

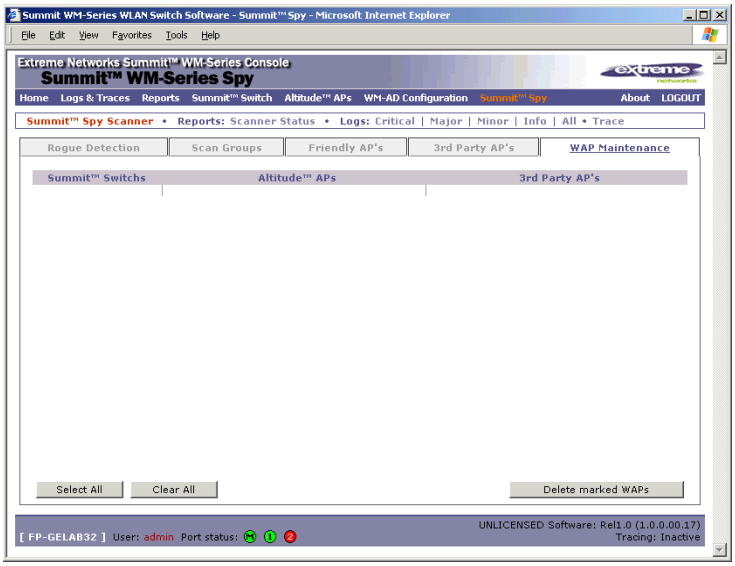
To view the list of the known third-party access points, click on the **3rd Party APs** tab. The *3rd Party APs* screen appears.


Summit WM-Series WLAN Switch Software - Summit™ Spy - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Extreme Networks Summit™ WM-Series Console
Summit™ WM-Series Spy
Home Logs & Traces Reports Summit™ Switch Altitude™ APs WM-AD Configuration Summit™ Spy About LOGOUT
Summit™ Spy Scanner • Reports: Scanner Status • Logs: Critical | Major | Minor | Info | All • Trace
Rogue Detection Scan Groups Friendly AP's 3rd Party AP's WAP Maintenance
3rd Party AP's
There are no 3rd party AP's found on the system
[FP-GELAB32] User: admin Port status:
UNLICENSED Software: Rel1.0 (1.0.0.00.17)
Tracing: Inactive

Maintain the Summit Spy list of access points and Altitude APs

When Altitude APs or Third-Party Access Points are deleted in the Summit WM-Series Switch Software user interface on a Summit WM-Series Switch has its RFDC running and is in communication with the Analysis Engine, this information will also be displayed in the Summit Spy's *AP Maintenance* screen.

1 To view the *AP Maintenance* screen, click on the **AP Maintenance** tab. The deleted access points and Altitude APs will be marked with a "Deleted" flag.


Summit WM-Series WLAN Switch Software - Summit™ Spy - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Extreme Networks Summit™ WM-Series Console
Summit™ WM-Series Spy
Home Logs & Traces Reports Summit™ Switch Altitude™ APs WM-AD Configuration Summit™ Spy About LOGOUT
Summit™ Spy Scanner • Reports: Scanner Status • Logs: Critical | Major | Minor | Info | All • Trace
Rogue Detection Scan Groups Friendly AP's 3rd Party AP's WAP Maintenance
Summit™ Switchs Altitude™ APs 3rd Party AP's
Select All Clear All Delete marked WAPs
[FP-GELAB32] User: admin Port status:
UNLICENSED Software: Rel1.0 (1.0.0.00.17)
Tracing: Inactive

2 To delete the marked access points and Altitude APs from the Summit Spy's database, click on the **Delete marked APs** button.

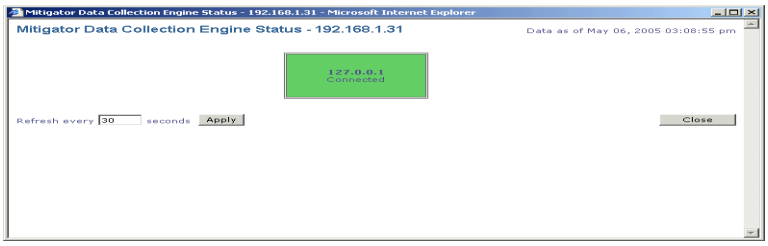
This will only delete them from the Summit Spy's database, not from the Summit WM-Series Switch's database.

Viewing the Scanner Status report

When the Summit Spy is enabled, you can view a report on the connection status of the RF Data Collector Engines with the Analysis Engine.

View the Summit Spy scanner engine status display

1 Click the **Summit Spy** tab in any screen, and then click on the **Scanner Status** tab. The Scanner Status report appears, as shown in the example below.


Mitigator Data Collection Engine Status - 192.168.1.31 - Microsoft Internet Explorer
Mitigator Data Collection Engine Status - 192.168.1.31
Data as of May 06, 2005 03:08:55 pm
127.0.0.1
Connected
Refresh every 30 seconds
Apply
Close

The boxes display the IP address of the RFDC engine, with status indicated by colour:

- Connected (green box) - the Analysis Engine has connection with the RFDC on that Summit WM-Series Switch.
- Connected but not serviced (yellow box) - the Analysis Engine has connection with the RFDC but is not synchronized with it yet.
- Not connected (red box) - the Analysis Engine is aware of the RFDC and attempting connection.

If no box appears, this means that the Analysis Engine is not trying to set up a connection with that RFDC Engine. Ensure that the RFDC address has been entered in the *Summit Spy Configuration* screen.

If the box appears red and remains red, ensure that the RFDC Engine is enabled on the appropriate Summit WM-Series Switch in the *Summit Spy Configuration* screen.

In the Logs - Traces screen, the Analysis Engine will appear as “Remote INS” and the RF Data Collection Engine will appear as RF Data Collector.

11 Ongoing operation

Altitude AP maintenance: software

Periodically, the software used by the Altitude APs is altered, either for reasons of upgrade or security. The new version of the software is installed from the Summit WM-Series Switch, using the *Altitude AP Maintenance* option.

You select the version of software for each Altitude AP that will be uploaded either immediately, or the next time the Altitude AP connects (part of the Altitude AP boot sequence is to seek and install its software from the Summit WM-Series Switch).

A number of the properties of each radio on a Altitude AP can be modified (in the *Altitude AP Configuration* screen) without requiring a reboot of the Altitude AP is also required after:

- enabling or disabling either radio, or changing the radio channel between "Auto" and any fixed channel number (in the *Altitude AP Configuration* screen)
- adding the Altitude AP to a WM-AD, or changing its radio assignment in a WM-AD (in the *WM-AD Configuration* screen)

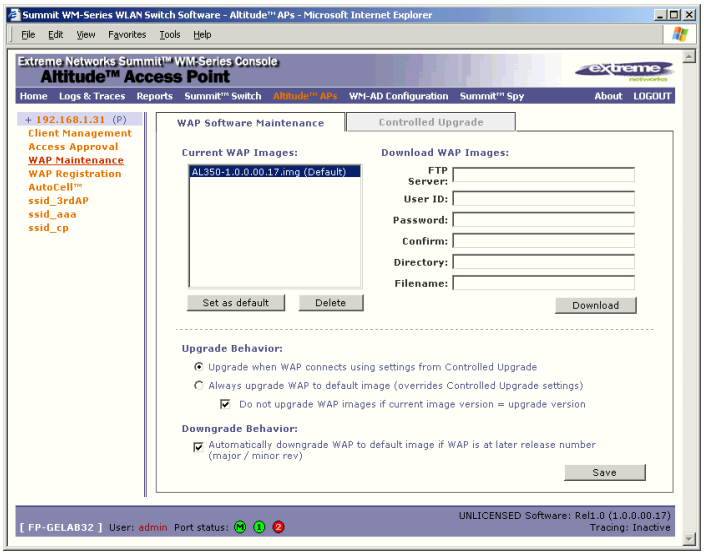
The Altitude AP keeps a backup copy of its software image. When a software upgrade is sent to the Altitude AP, the upgrade becomes the Altitude AP's current image and the previous image becomes the backup. In the event of failure of the current image, the Altitude AP will run the backup image.

Maintain the list of current Altitude AP software images

1 Click on the **Altitude APs** tab. The *Altitude AP Configuration* screen appears. Click on the **AP Maintenance** option.

2 Click on the **AP Software Maintenance** tab. The *AP Software Maintenance* screen appears.

The **Current AP Images** area displays the list of AP software versions that have been downloaded and are available. (This list appears in the drop-down list of available images in the *Controlled Upgrade* screen.)



3 To select an image as the default image to be used for software upgrade, highlight the image name in the list and click on the **Set as default** button.

4 To delete a software image from the list, highlight the version in the displayed list of **Current AP Images** and click on the **Delete** button.

5 To download a new image to be added to the list, fill in the fields in the **Download AP Images** area with parameters for FTP transfer: **FTP server**, **User ID**, **Password**, **Confirm password**, **Directory**, **Filename**. Click on the **Download** button.

6 In the **Upgrade Behavior** area, select one of these radio buttons:

- Upgrade when AP connects using setting from Controlled Upgrade
- Always upgrade AP to default image (overrides Controlled Upgrade settings)

For either choice, click the checkbox on to prevent an upgrade if current image version is the same as the upgrade version (this overrides Upgrade Now behavior)

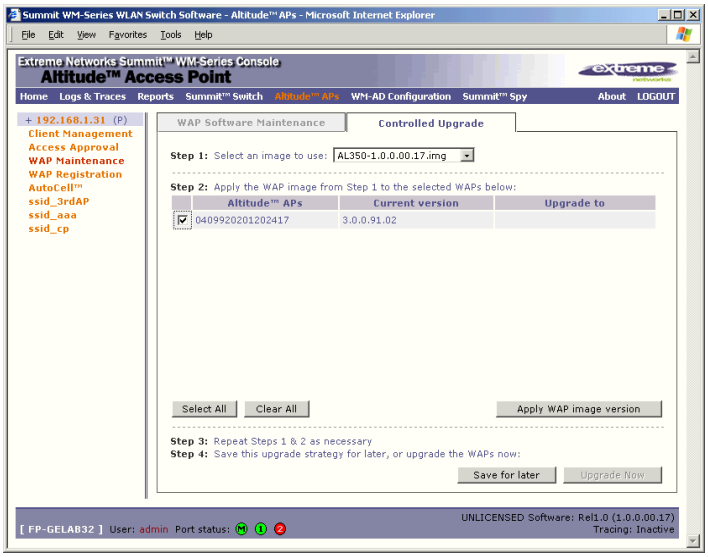
7 In the **Downgrade Behavior** area, click the checkbox on to automatically downgrade the AP to the default image if AP is at later release number (major/minor rev)

8 To save these parameters, click on the **Save** button.

Define parameters for a Altitude AP controlled software upgrade.

1 Click on the **Altitude APs** tab. The *Altitude AP Configuration* screen appears. Click on the **AP Maintenance** option.

2 Click on the **Controlled Upgrade** tab. The *Controlled Upgrade* screen appears.


Summit WM-Series WLAN Switch Software - Altitude™ APs - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Extreme Networks Summit™ WM-Series Console
Altitude™ Access Point
Home Logs & Traces Reports Summit™ Switch Altitude™ APs WM-AD Configuration Summit™ Spy About LOGOUT
+ 192.168.1.31 (P)
Client Management
Access Approval
WAP Maintenance
WAP Registration
AutoCell™
ssid_3rdAP
ssid_aaa
ssid_cp
WAP Software Maintenance
Controlled Upgrade
Step 1: Select an image to use: AL350-1.0.0.00.17.img
Step 2: Apply the WAP image from Step 1 to the selected WAPs below:
Altitude™ APs
Current version
Upgrade to
0409920201202417
3.0.0.91.02
Select All
Clear All
Apply WAP image version
Step 3: Repeat Steps 1 & 2 as necessary
Step 4: Save this upgrade strategy for later, or upgrade the WAPs now:
Save for later
Upgrade Now
[FP-GELAB32] User: admin Port status:
UNLICENSED Software: Rel1.0 (1.0.0.00.17)
Tracing: Inactive

The screen displays the steps to initiate a software upgrade.

3 **Step 1**: From the drop-down list, select the software version you wish to use for the upgrade. (This list is maintained in the *AP Software Maintenance* screen.)

4 **Step 2**: In the list of the registered Altitude APs and the current software image on each one, select a Altitude AP for software upgrade by clicking its checkbox on. Use the Select All or Clear All buttons to modify your selections.

5 **Step 3**: Click on Apply AP image version button. The selected software image from Step 1 now appears in the Upgrade To column beside the selected Altitude AP.

6 **Step 4**: To save the software upgrade strategy so that you run it later, click on the Save for later button, or,

To run the software upgrade immediately, click on the **Upgrade Now** button. This will force the selected Altitude AP to reboot, and the new software version will be loaded during this process. The "Always upgrade AP to default image" choice in the *AP Software Maintenance* screen overrides Controlled Upgrade settings.

Altitude AP client management

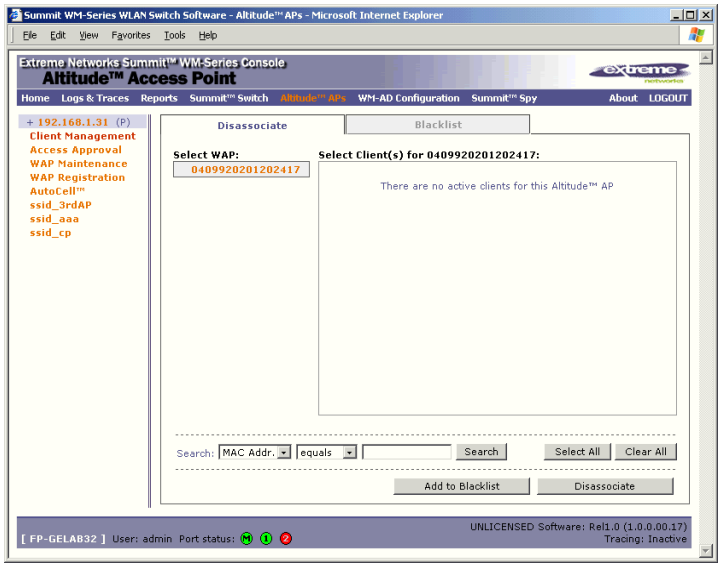
There are times when you want to cut the connection with a particular wireless device, for service reasons or to deal with a security issue. Using the Altitude AP Client Management screen, you can view all the associated wireless devices, by MAC address, on a selected Altitude AP. Then you can then:

- disassociate a selected wireless device from its Altitude AP.
- add a selected wireless device's MAC address to a Blacklist of wireless clients that will not be allowed to associate with the Altitude AP.

Client disassociate

Disassociate a wireless device client

1 Click on the **Altitude APs** tab. Click on the **Client Management** option. Click on the **Disassociate** tab. The *Disassociate* screen appears.


Summit WM-Series WLAN Switch Software - Altitude™ APs - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Extreme Networks Summit™ WM-Series Console
Altitude™ Access Point
Home Logs & Traces Reports Summit™ Switch Altitude™ APs WM-AD Configuration Summit™ Spy About LOGOUT
+ 192.168.1.31 (P)
Client Management
Access Approval
WAP Maintenance
WAP Registration
AutoCell™
ssid_3rdAP
ssid_aaa
ssid_cp
Disassociate
Blacklist
Select WAP:
0409920201202417
Select Client(s) for 0409920201202417:
There are no active clients for this Altitude™ AP
Search: MAC Addr. equals Search Select All Clear All
Add to Blacklist Disassociate
[FP-GELAB32] User: admin Port status:
UNLICENSED Software: Rel1.0 (1.0.0.00.17)
Tracing: Inactive

2 Click on the checkbox to select the wireless device to be disassociated.

3 To search for a client by MAC Address, IP Address or User ID, select the search parameters from the pull-down list. Then key in the search string and click on the **Search** button. (Wildcard searches are supported.)

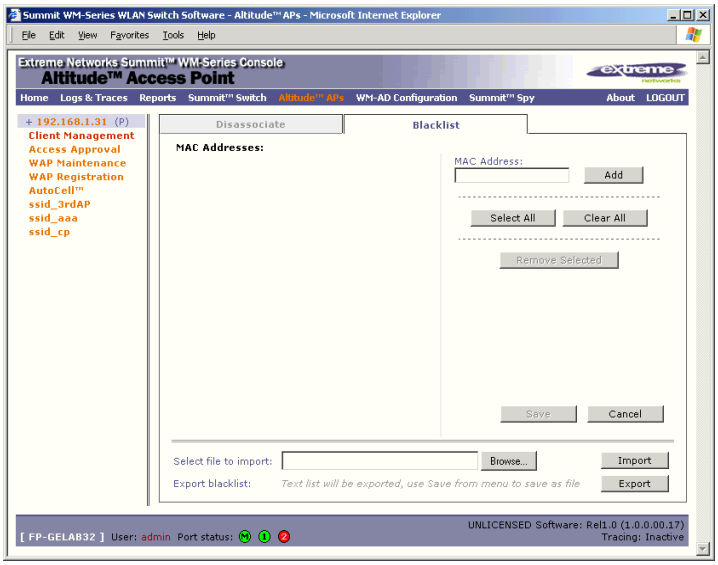
4 Click on the **Add to blacklist** button to add the selected wireless client's MAC address to the blacklist (see next topic).

5 Click on the **Disassociate** button to terminate the client's session immediately.

Client blacklist

Add a wireless device client to a blacklist

1 Click on the **Client Management** option in the *Altitude AP Configuration* screen. Click on the **Blacklist** tab. The *Blacklist* screen appears.



The *Blacklist* screen displays the current list of MAC addresses that will be not be allowed to associate. Clients selected in the *Disassociate* screen for the Blacklist will appear here.

2 To add a new MAC address to the Blacklist, key it in the MAC Address field and click on the **Add** button. It will appear in the list of addresses on the left.

3 To clear an address from the Blacklist, click its checkbox on, and then click on the **Remove Selected** button.

4 To save the amended Blacklist, click on the **Save** button.

5 To import a list of MAC addresses for the Blacklist, key in or brows for the file name, and then click on the **Import** button.

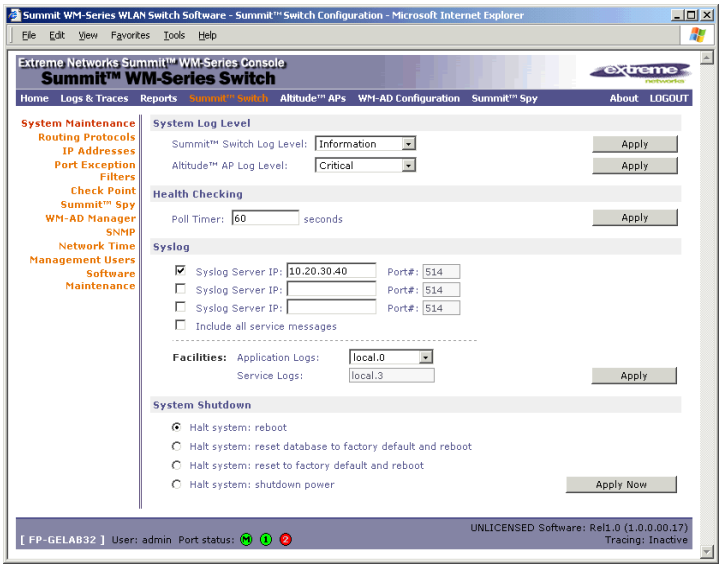
6 To export the current Blacklist, first use the File menu Save option to save the file, and then click on the Summit WM-Series Switch system maintenance.

Use the *System Maintenance* screen to perform various maintenance tasks, including:

- change the log level
- set a poll interval for checking the status of the Altitude APs (“Health Checking”)
- force an immediate system shutdown, with or without reboot
- enable and define parameters for Syslog event reporting.

Syslog event reporting uses the *syslog protocol* to relay event messages to a centralized event server on your enterprise network. In the protocol a device generates messages, a relay receives and forwards the messages, and a collector (a syslog server) receives the messages without relaying them.

1 Click on the **Summit WM-Series Switch** tab. Click on the **System Maintenance** option. The *System Maintenance* screen appears.



Health Checking

1 In the **Poll Interval** field, key in a time in seconds for the Summit WM-Series Switch to check that the Altitude APs are still there. Click on the **Apply** button.

Force a system shutdown on the Summit WM-Series Switch

1 To shut down the Summit WM-Series Switch Software system, with its Altitude APs, click on the appropriate radio button:

- Halt system, reboot
- Halt system, reset database to factory default and reboot
- Halt system, reset to factory default and reboot
- Halt system, shutdown power

2 Click on the **Apply Now** button.

Change the system log level

1 From the **Log Level** drop-down list, select the desired log level (Trace, Info, Minor, Major, Critical). Click on the **Apply** button.

Enable and configure Syslog

1 Click the checkbox on to enable the **Syslog** function for up to three syslog servers.

2 For each enabled syslog server, key in a valid IP address for the server on the network. The default port for syslog is 514.

3 In the **Facilities** area, in the **Application Logs** drop-down list, select the log level (“local.0” to “local.6”) to be sent to the syslog server. (This will apply to all three servers.)

4 To include additional system messages, click the **Include all service messages** checkbox on. If the box is left unchecked, only component messages (logs and traces) are relayed. (This will apply to all three servers.) The additional system messages are:

- DHCP messages reporting users receiving IP addresses
- Startup Manager Task messages reporting component startup and failure

If you clicked the **Include all service messages** checkbox on, the **Facilities** drop-down list for **Service Logs** become selectable. Select a log level from the list.

5 To activate the above settings, click on the **Apply** button.

NOTE

The syslog daemon must be running on both the Summit WM-Series Switch and on the remote syslog server before the logs can be synchronized. If you change the log level on the Summit WM-Series Switch, you must also modify the appropriate setting in the syslog configuration on remote syslog server.

Syslog and Summit WM-Series Switch Software event log mapping is shown below:

Syslog	Summit WM-Series Switch Software
LOG_CRIT	Critical
LOG_ERR	Major
LOG_WARNING	Minor
LOG_INFO	Information
LOG_DEBUG	Trace

Summit WM-Series Switch software maintenance

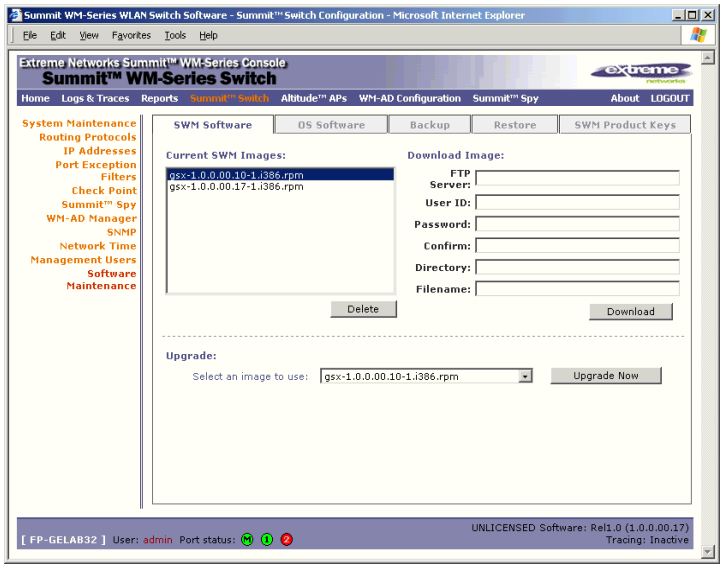
You can update the core Summit WM-Series Switch software files, and the Operating System (OS) software using the Software Maintenance function in the Summit WM-Series Switch Configuration area of the user interface. This function is also provided in the Command Line Interface (CLI). See Appendix , “CLI command reference”.

A facility to backup and restore the Summit WM-Series Switch database will also be available in the GUI user interface and in the Command Line Interface (CLI).

The maintenance interface also includes the product key maintenance, for first-time setup and upgrades, if appropriate. See “Enabling the product key” on page 31.

Upgrade the Summit WM-Series Switch software

1 Click on the **Summit WM-Series Switch** tab. Click on the **Software Maintenance** option. Click on the **SWM Software Maintenance** tab. The *Software Maintenance* screen appears.



The **Current SWM Images** area displays the list of software versions that have been downloaded and are available. (This list appears in the drop-down list of available images in the **Upgrade** area.)

2 To select an image as the default image to be used for software upgrade, highlight the image name in the list and click on the **Set as default** button.

3 To delete a software image from the list, highlight the version in the displayed list of **Current SWM Images** and click on the **Delete** button.

4 To download a new image to be added to the list, fill in the fields in the **Download SWM Images** area with parameters for FTP transfer: **FTP server**, **User ID**, **Password**, **Confirm password**, **Directory**, **Filename**.

5 Click on the **Download** button.

6 In the **Upgrade** area, select an image from the drop-down list.

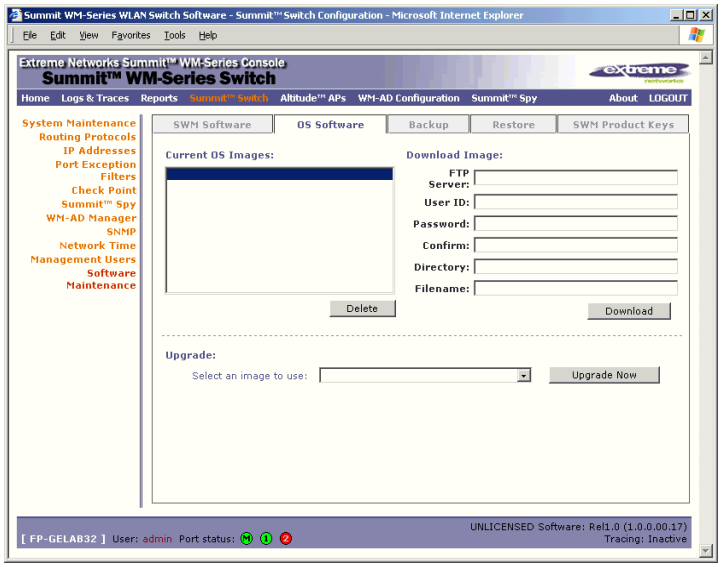
7 To launch the upgrade with the selected image, click on the **Upgrade Now** button.

8 In the dialog box that appears, confirm the upgrade.

At this point, all sessions will be logged. The previous software will be uninstalled automatically. The new software will be installed. The Summit WM-Series Switch will reboot automatically. The database will be updated and migrated behind the scenes.

Upgrade the Operating System software

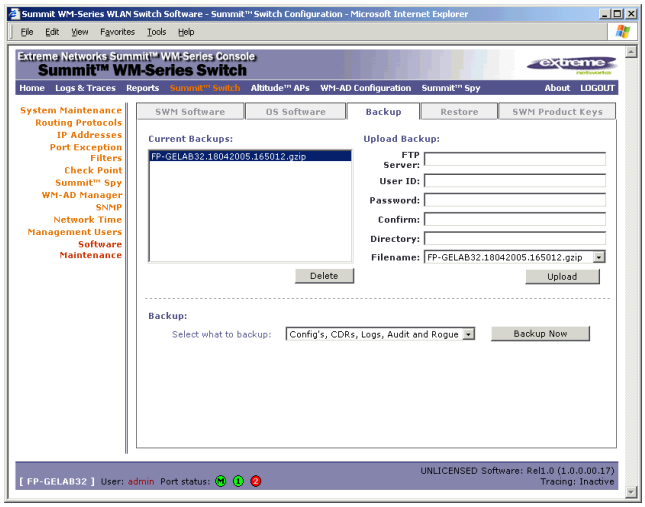
1 Click on the **Summit WM-Series Switch** tab. Click on the **Software Maintenance** option. Click on the **OS Software** tab. The *OS Software Maintenance screen* appears.



2 Follow the steps described for the *Software Maintenance* screen.

Back up the Summit WM-Series Switch software

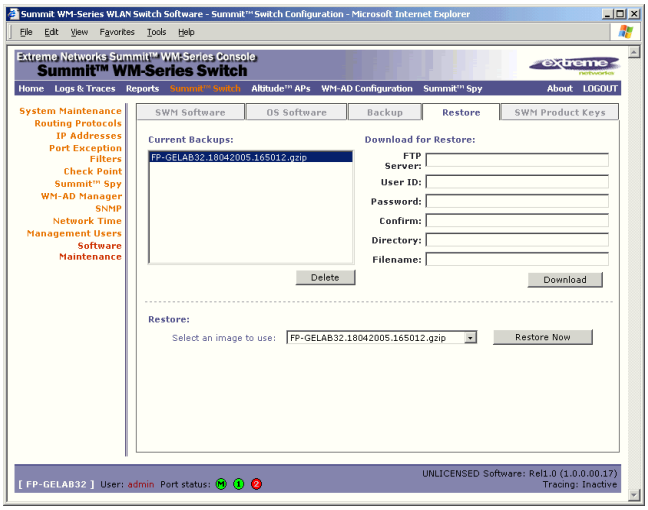
1 Click on the **Summit WM-Series Switch** tab. Click on the **Software Maintenance** option. Click on the **Backup** tab. The *Backup* screen appears.



2 Follow the steps described for the *Software Maintenance* screen. In the **Backup** area, select what to backup from the drop-down list.

Restore the Summit WM-Series Switch software

1 Click on the **Summit WM-Series Switch** tab. Click on the **Software Maintenance** option. Click on the **Restore** tab. The *Restore* screen appears.



2 Follow the steps described for the *Software Maintenance* screen.

Summit WM-Series Switch Software logs and traces

Summit WM-Series Switch Software log and data files

The Summit WM-Series Switch Software system stores configuration data and log files. These files include:

- event and alarm logs (triggered by events, described below)
- trace logs (triggered by component activity, described below)
- accounting files (created on a half-hourly basis, up to six files)

The files are stored in the operating system and have a maximum size of 1 GB.

The accounting files are stored in flat files in a directory that is created every day. Eight directories are maintained in a circular buffer (when all are full, the most recent replaces the earliest).

Viewing log, alarm and trace messages

To view the logs and traces, select the **Logs & Traces** tab. The Summit WM-Series Switch generates three types of messages:

- Logs (including alarms): messages that are triggered by events
- Traces: messages that display activity by component, for system debugging, troubleshooting and internal monitoring of software
- Audits: files that record administrative changes made to the system (the GUI Audit displays changes to the Graphical User Interface on the Summit WM-Series Switch)

Logs and alarms

The log messages contain the time of event, severity, source component and any details generated by the source component. The messages are classified at four levels of severity:

- Informational, the activity of normal operation
- Minor (alarm)
- Major (alarm)
- Critical (alarm)

The alarm messages (minor, major or critical log messages) are triggered by activities that meet certain conditions that should be known and dealt with.

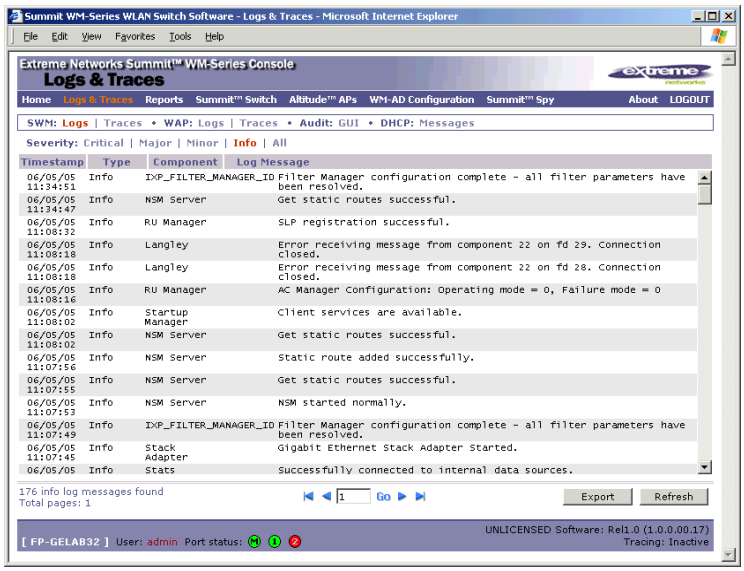
Examples of events on the Summit WM-Series Switch that generate an alarm message:

- Reboot due to failure
- Software upgrade failure on the Summit WM-Series Switch
- Software upgrade failure on the Altitude AP
- Detection of rogue access point activity without valid ID

If SNMP is enabled on the Summit WM-Series Switch, alarm conditions will trigger a trap in SNMP (Simple Network Management Protocol). An SNMP trap is an event notification sent by the managed agent (a network device) to the management system to identify the occurrence of conditions. (See "Setting up SNMP" on page 115 for more information on enabling this function on the Summit WM-Series Switch).

View the Logs

1 Click on the **Logs & Traces** tab. In the Navigation bar, click on one of the **Log** tabs. The selected *Log* screen appears:


Summit WM-Series WLAN Switch Software - Logs & Traces - Microsoft Internet Explorer
Extreme Networks Summit™ WM-Series Console
Logs & Traces
Home Logs & Traces Reports Summit™ Switch Altitude™ APs WM-AD Configuration Summit™ Spy About LOGOUT
SWM: Logs | Traces • WAP: Logs | Traces • Audit: GUI • DHCP: Messages
Severity: Critical | Major | Minor | Info | All
Timestamp Type Component Log Message
06/05/05 11:34:51 Info IXP_FILTER_MANAGER_ID Filter Manager configuration complete - all filter parameters have been resolved.
06/05/05 11:34:47 Info NSM Server Get static routes successful.
06/05/05 11:08:32 Info RU Manager SLP registration successful.
06/05/05 11:08:18 Info Langley Error receiving message from component 22 on fd 29. Connection closed.
06/05/05 11:08:18 Info Langley Error receiving message from component 22 on fd 28. Connection closed.
06/05/05 11:08:16 Info RU Manager AC Manager Configuration: Operating mode = 0, Failure mode = 0
06/05/05 11:08:02 Info Startup Manager Client services are available.
06/05/05 11:08:02 Info NSM Server Get static routes successful.
06/05/05 11:07:56 Info NSM Server Static route added successfully.
06/05/05 11:07:55 Info NSM Server Get static routes successful.
06/05/05 11:07:53 Info NSM Server NSM started normally.
06/05/05 11:07:49 Info IXP_FILTER_MANAGER_ID Filter Manager configuration complete - all filter parameters have been resolved.
06/05/05 11:07:45 Info Stack Adapter Gigabit Ethernet Stack Adapter Started.
06/05/05 Info Stats Successfully connected to internal data sources.
176 info log messages found
Total pages: 1
Go
Export
Refresh
UNLICENSED Software: Rel1.0 (1.0.0.00.17)
[FP-GELAB32] User: admin Port status:
Tracing: Inactive

The events are displayed in chronological order, sorted by the **Timestamp** column.

2 To sort the display by **Type** or **Component**, click on the column heading.

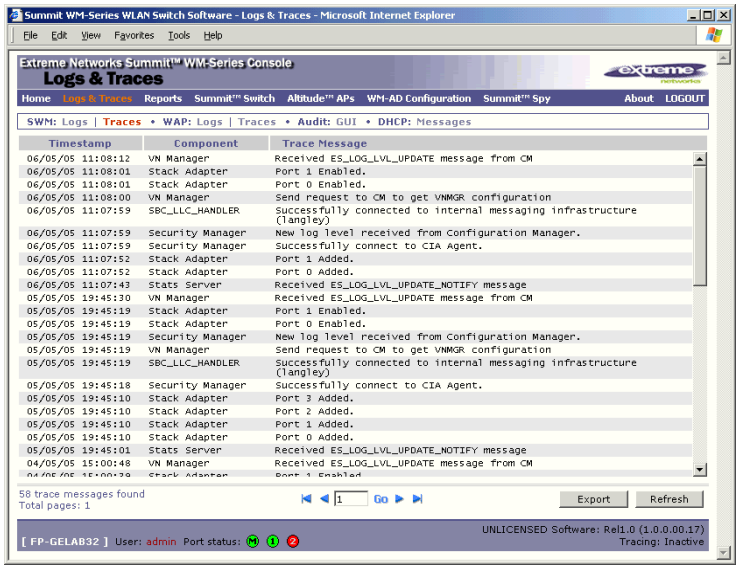
3 To filter the logs by severity, in order to display only **Info**, **Minor**, **Major**, or **Critical** logs, click on the appropriate **Log** tab at the top of the screen.

4 To refresh the information in any display, click on the **Refresh** button.

5 To export information from a display as an HTML file, click on the **Export to HTML** button.

View the Traces

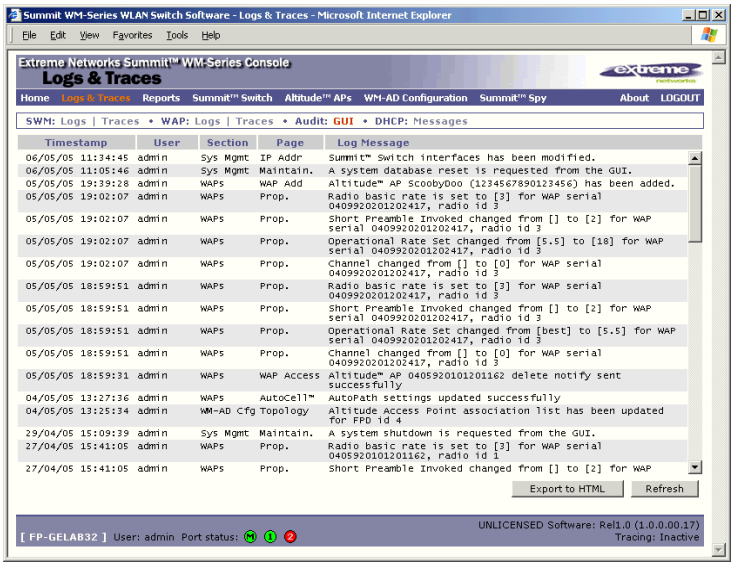
1 To view the list of **Traces**, messages by component, click on its tab.


Summit WM-Series WLAN Switch Software - Logs & Traces - Microsoft Internet Explorer
Extreme Networks Summit™ WM-Series Console
Logs & Traces
Home Logs & Traces Reports Summit™ Switch Altitude™ APs WM-AD Configuration Summit™ Spy About LOGOUT
SWM: Logs | Traces • WAP: Logs | Traces • Audit: GUI • DHCP: Messages
Timestamp Component Trace Message
06/05/05 11:08:12 VN Manager Received ES_LOG_LVL_UPDATE message from CM
06/05/05 11:08:01 Stack Adapter Port 1 Enabled.
06/05/05 11:08:01 Stack Adapter Port 0 Enabled.
06/05/05 11:08:00 VN Manager Send request to CM to get VNMGR configuration
06/05/05 11:07:59 SBC_LLC_HANDLER Successfully connected to internal messaging infrastructure (langley)
06/05/05 11:07:59 Security Manager New log level received from Configuration Manager.
06/05/05 11:07:59 Security Manager Successfully connect to CIA Agent.
06/05/05 11:07:52 Stack Adapter Port 1 Added.
06/05/05 11:07:52 Stack Adapter Port 0 Added.
06/05/05 11:07:43 Stats Server Received ES_LOG_LVL_UPDATE_NOTIFY message
05/05/05 19:45:30 VN Manager Received ES_LOG_LVL_UPDATE message from CM
05/05/05 19:45:19 Stack Adapter Port 1 Enabled.
05/05/05 19:45:19 Stack Adapter Port 0 Enabled.
05/05/05 19:45:19 Security Manager New log level received from Configuration Manager.
05/05/05 19:45:19 VN Manager Send request to CM to get VNMGR configuration
05/05/05 19:45:19 SBC_LLC_HANDLER Successfully connected to internal messaging infrastructure (langley)
05/05/05 19:45:18 Security Manager Successfully connect to CIA Agent.
05/05/05 19:45:10 Stack Adapter Port 3 Added.
05/05/05 19:45:10 Stack Adapter Port 2 Added.
05/05/05 19:45:10 Stack Adapter Port 1 Added.
05/05/05 19:45:10 Stack Adapter Port 0 Added.
05/05/05 19:45:01 Stats Server Received ES_LOG_LVL_UPDATE_NOTIFY message
04/05/05 15:00:48 VN Manager Received ES_LOG_LVL_UPDATE message from CM
58 trace messages found
Total pages: 1
Go
Export
Refresh
UNLICENSED Software: Rel1.0 (1.0.0.00.17)
[FP-GELAB32] User: admin Port status:
Tracing: Inactive

You can sort, refresh and export the Trace information, as described for Log displays.

View the Audits

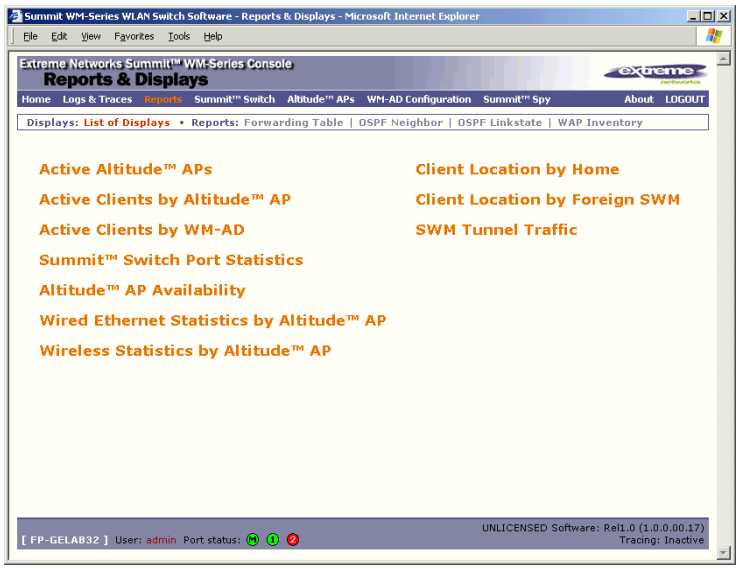
1 To view the **GUI Audit** display, click on the **GUI Audit** tab.


Summit WM-Series WLAN Switch Software - Logs & Traces - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Extreme Networks Summit™ WM-Series Console
Logs & Traces
Home Logs & Traces Reports Summit™ Switch Altitude™ APs WM-AD Configuration Summit™ Spy About LOGOUT
SWM: Logs | Traces • WAP: Logs | Traces • Audit: GUI • DHCP: Messages
Timestamp User Section Page Log Message
06/05/05 11:34:45 admin Sys Mgmt IP Addr Summit™ Switch interfaces has been modified.
06/05/05 11:05:46 admin Sys Mgmt Maintain. A system database reset is requested from the GUI.
05/05/05 19:39:28 admin WAPs WAP Add Altitude™ AP ScoobyDoo (12345678901234567) has been added.
05/05/05 19:02:07 admin WAPs Prop. Radio basic rate is set to [3] for WAP serial 0409920201202417, radio id 3
05/05/05 19:02:07 admin WAPs Prop. Short Preamble Invoked changed from [] to [2] for WAP serial 0409920201202417, radio id 3
05/05/05 19:02:07 admin WAPs Prop. Operational Rate Set changed from [5.5] to [18] for WAP serial 0409920201202417, radio id 3
05/05/05 19:02:07 admin WAPs Prop. Channel changed from [] to [0] for WAP serial 0409920201202417, radio id 3
05/05/05 18:59:51 admin WAPs Prop. Radio basic rate is set to [3] for WAP serial 0409920201202417, radio id 3
05/05/05 18:59:51 admin WAPs Prop. Short Preamble Invoked changed from [] to [2] for WAP serial 0409920201202417, radio id 3
05/05/05 18:59:51 admin WAPs Prop. Operational Rate Set changed from [best] to [5.5] for WAP serial 0409920201202417, radio id 3
05/05/05 18:59:51 admin WAPs Prop. Channel changed from [] to [0] for WAP serial 0409920201202417, radio id 3
05/05/05 18:59:31 admin WAPs WAP Access Altitude™ AP 0405920101201162 delete notify sent successfully
04/05/05 13:27:36 admin WAPs AutoCell™ AutoPath settings updated successfully
04/05/05 13:25:34 admin WM-AD Cfg Topology Altitude Access Point association list has been updated for FPD id 4
29/04/05 15:09:39 admin Sys Mgmt Maintain. A system shutdown is requested from the GUI.
27/04/05 15:41:05 admin WAPs Prop. Radio basic rate is set to [3] for WAP serial 0405920101201162, radio id 1
27/04/05 15:41:05 admin WAPs Prop. Short Preamble Invoked changed from [] to [2] for WAP
Export to HTML
Refresh
UNLICENSED Software: Rel1.0 (1.0.0.00.17)
[FP-GELAB32] User: admin Port status:
Tracing: Inactive

Reports and displays

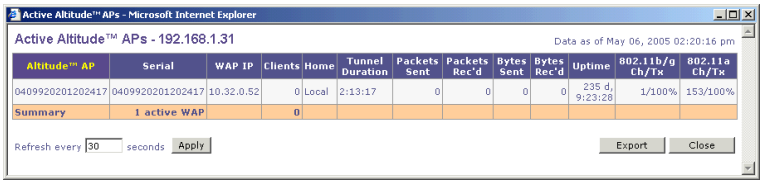
View displays

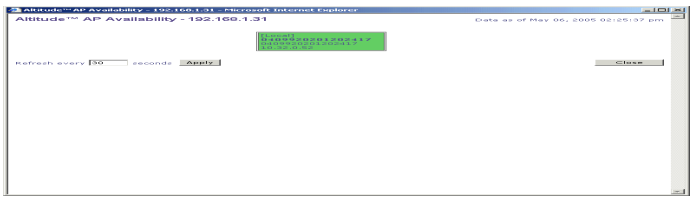
To view Summit WM-Series Switch Software reports and displays, click on the **Reports** tab. The *List of Displays* screen appears, with a menu of available displays.


Summit WM-Series WLAN Switch Software - Reports & Displays - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Extreme Networks Summit™ WM-Series Console
Reports & Displays
Home Logs & Traces Reports Summit™ Switch Altitude™ APs WM-AD Configuration Summit™ Spy About LOGOUT
Displays: List of Displays • Reports: Forwarding Table | OSPF Neighbor | OSPF Linkstate | WAP Inventory
Active Altitude™ APs
Active Clients by Altitude™ AP
Active Clients by WM-AD
Summit™ Switch Port Statistics
Altitude™ AP Availability
Wired Ethernet Statistics by Altitude™ AP
Wireless Statistics by Altitude™ AP
Client Location by Home
Client Location by Foreign SWM
SWM Tunnel Traffic
[FP-GELAB32] User: admin Port status:
UNLICENSED Software: Rel1.0 (1.0.0.00.17)
Tracing: Inactive

The three options on the right-hand side of the screen appear only if the WM-AD Manager function has been enabled.

Click on an option in the menu to view its display screen (examples below):





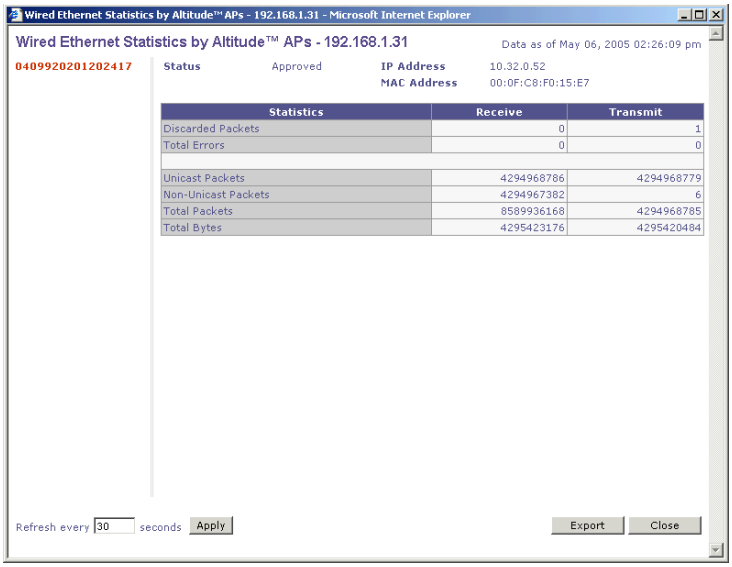
View statistics for Altitude APs

Two displays are snapshots of activity at that point in time on a selected Altitude AP:

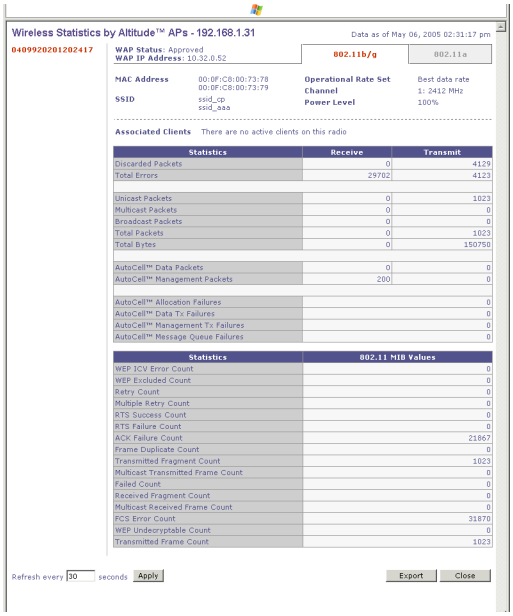
- Wired Ethernet Statistics by Altitude APs
- Wireless Statistics by Altitude APs

The statistics displayed are those defined in the 802.11 MIB, in the IEEE 802.11 standard.

In the **Wired Ethernet Statistics by Altitude APs** display, click on one of the registered Altitude APs to display its information.


Wired Ethernet Statistics by Altitude™ APs - 192.168.1.31 - Microsoft Internet Explorer
Wired Ethernet Statistics by Altitude™ APs - 192.168.1.31
Data as of May 06, 2005 02:26:09 pm
0409920201202417
Status Approved
IP Address 10.32.0.52
MAC Address 00:0F:C8:F0:15:E7
Statistics Receive Transmit
Discarded Packets 0 1
Total Errors 0 0
Unicast Packets 4294968786 4294968779
Non-Unicast Packets 4294967382 6
Total Packets 8589936168 4294968785
Total Bytes 4295423176 4295420484
Refresh every 30 seconds Apply
Export Close

To view the **Wireless Statistics by Altitude APs** display, click on its option in the **List of Displays** menu.


Wireless Statistics by Altitude™ APs - 192.168.1.31
Data as of May 06, 2005 02:31:17 pm
0409920201202417
WAP Status: Approved
WAP IP Address: 10.32.0.52
802.11b/g
802.11a
MAC Address 00:0F:C8:00:73:78 00:0F:C8:00:73:79
SSID ssid_cp ssid_aaa
Operational Rate Set Best data rate
Channel 1: 2412 MHz
Power Level 100%
Associated Clients There are no active clients on this radio
Statistics Receive Transmit
Discarded Packets 0 4129
Total Errors 29702 4123
Unicast Packets 0 1023
Multicast Packets 0 0
Broadcast Packets 0 0
Total Packets 0 1023
Total Bytes 0 150750
AutoCell™ Data Packets 0 0
AutoCell™ Management Packets 200 0
AutoCell™ Allocation Failures 0
AutoCell™ Data Tx Failures 0
AutoCell™ Management Tx Failures 0
AutoCell™ Message Queue Failures 0
Statistics 802.11 MIB Values
WEP ICV Error Count 0
WEP Excluded Count 0
Retry Count 0
Multiple Retry Count 0
RTS Success Count 0
RTS Failure Count 0
ACK Failure Count 21867
Frame Duplicate Count 0
Transmitted Fragment Count 1023
Multicast Transmitted Frame Count 0
Failed Count 0
Received Fragment Count 0
Multicast Received Frame Count 0
FCS Error Count 31870
WEP Undecryptable Count 0
Transmitted Frame Count 1023
Refresh every 30 seconds Apply
Export Close

The displays lists the registered Altitude APs Click on the selected Altitude AP. Then click on the appropriate tab to display information for each radio on the Altitude AP.

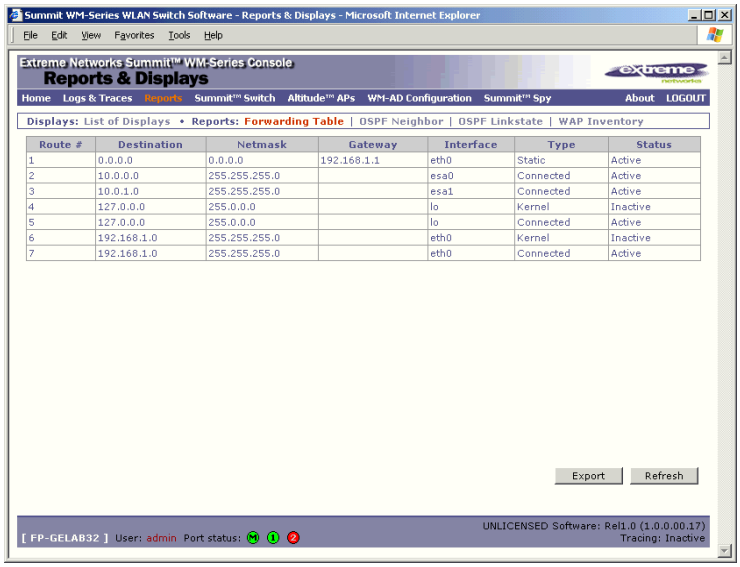
If there are associated clients on this radio, you can view information on a selected client. Click on the **View Client** button. The *Associated Clients* popup window appears.

View reports

To view Summit WM-Series Switch Software reports and displays, click on the **Reports** tab. The *List of Displays* screen appears. To access a report, click on one of the options in the navigation bar. The following reports are currently available in Summit WM-Series Switch Software:

- Forwarding Table (routes defined in the Summit WM-Series Switch Routing Protocols screen)
- OSPF Neighbor (if OSPF is enabled in the Routing Protocols screen)
- OSPF Linkstate (if OSPF is enabled in the Routing Protocols screen)
- AP Inventory (a consolidated summary of Altitude AP setup)

An example of a report is shown below:


Summit WM-Series WLAN Switch Software - Reports & Displays - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Extreme Networks Summit™ WM-Series Console
Reports & Displays
Home Logs & Traces Reports Summit™ Switch Altitude™ APs WM-AD Configuration Summit™ Spy About LOGOUT
Displays: List of Displays • Reports: Forwarding Table | OSPF Neighbor | OSPF Linkstate | WAP Inventory
Route # Destination Netmask Gateway Interface Type Status
1 0.0.0.0 0.0.0.0 192.168.1.1 eth0 Static Active
2 10.0.0.0 255.255.255.0 esa0 Connected Active
3 10.0.1.0 255.255.255.0 esa1 Connected Active
4 127.0.0.0 255.0.0.0 lo Kernel Inactive
5 127.0.0.0 255.0.0.0 lo Connected Active
6 192.168.1.0 255.255.255.0 eth0 Kernel Inactive
7 192.168.1.0 255.255.255.0 eth0 Connected Active
Export
Refresh
[FP-GELAB32] User: admin Port status:
UNLICENSED Software: Rel1.0 (1.0.0.00.17)
Tracing: Inactive

Glossary

Networking terms and abbreviations

A

AAA
Authentication, Authorization and Accounting. A system in IP-based networking to control what computer resources users have access to and to keep track of the activity of users over a network.

Access Point (AP)
A wireless LAN transceiver or "base station" that can connect a wired LAN to one or many wireless devices.

Ad-hoc mode
An 802.11 networking framework in which devices or stations communicate directly with each other, without the use of an access point (AP). (Compare Infrastructure Mode)

AES
Advanced Encryption Standard (AES) is an algorithm for encryption that works at multiple network layers simultaneously. As a block cipher, AES encrypts data in fixed-size blocks of 128 bits. AES was created by the National Institute of Standards and Technology (NIST). AES is a privacy transform for IPSec and Internet Key Exchange (IKE). AES has a variable key length - the algorithm can specify a 128-bit key (the default), a 192-bit key, or a 256-bit key.

For the WPA2/802.11i implementation of AES, a 128 bit key length is used. AES encryption includes 4 stages that make up one round. Each round is then iterated 10, 12 or 14 times depending upon the bit-key size. For the WPA2/802.11i implementation of AES, each round is iterated 10 times.

AES-CCMP
AES uses the Counter-Mode/CBC-MAC Protocol (CCMP). CCM is a new mode of operation for a block cipher that enables a single key to be used for both encryption and authentication. The two underlying modes employed in CCM include Counter mode (CTR) that achieves data encryption and Cipher Block Chaining Message Authentication Code (CBC-MAC) to provide data integrity.

ARP
Address Resolution Protocol. A protocol used to obtain the physical addresses (such as MAC addresses) of hardware units in a network environment. A host obtains such a physical address by broadcasting an ARP request, which contains the IP address of the target hardware unit. If the request finds a unit with that IP address, the unit replies with its physical hardware address.

Association
A connection between a wireless device and an Access Point.

asynchronous
Asynchronous transmission mode (ATM). A start/stop transmission in which each character is preceded by a start signal and followed by one or more stop signals. A variable time interval can exist between characters. ATM is the preferred technology for the transfer of images.

B

BSS

Basic Service Set. A wireless topology consisting of one Access Point connected to a wired network and a set of wireless devices. Also called an infrastructure network. *See also* IBSS.

C

Captive Portal

A browser-based authentication mechanism that forces unauthenticated users to a web page. Sometimes called a "reverse firewall".

CDR

Call Data (Detail) Record

In Internet telephony, a call detail record is a data record that contains information related to a telephone call, such as the origination and destination addresses of the call, the time the call started and ended, the duration of the call, the time of day the call was made and any toll charges that were added through the network or charges for operator services, among other details of the call.

In essence, call accounting is a database application that processes call data from your switch (PBX, iPBX, or key system) via a CDR (call detail record) or SMDR (station message detail record) port. The call data record details your system's incoming and outgoing calls by thresholds, including time of call, duration of call, dialing extension, and number dialed. Call data is stored in a PC database

CHAP

Challenge-Handshake Authentication Protocol. One of the two main authentication protocols used to verify a user's name and password for PPP Internet connections. CHAP is more secure than PAP because it performs a three-way handshake during the initial link establishment between the home and remote machines. It can also repeat the authentication anytime after the link has been established.

CLI

Command Line Interface.

Collision

Two Ethernet packets attempting to use the medium simultaneously. Ethernet is a shared media, so there are rules for sending packets of data to avoid conflicts and protect data integrity. When two nodes at different locations attempt to send data at the same time, a collision will result. Segmenting the network with bridges or switches is one way of reducing collisions in an overcrowded network.

D

Datagram

A datagram is "a self-contained, independent entity of data carrying sufficient information to be routed from the source to the destination computer without reliance on earlier exchanges between this source and destination computer and the transporting network." (RFC1594). The term has been generally replaced by the term packet. Datagrams or packets are the message units that the Internet Protocol deals with and that the Internet transports.

Decapsulation

See tunnelling.

D (Continued)

Device Server

A specialized, network-based hardware device designed to perform a single or specialized set of server functions. Print servers, terminal servers, remote access servers and network time servers are examples of device servers.

DHCP

Dynamic Host Configuration Protocol. A protocol for assigning dynamic IP addresses to devices on a network. With dynamic addressing, a device can have a different IP address every time it connects to the network. In some systems, the device's IP address can even change while it is still connected. DHCP also supports a mix of static and dynamic IP addresses.

DHCP consists of two components: a protocol for delivering host-specific configuration parameters from a DHCP server to a host and a mechanism for allocation of network addresses to hosts. (IETF RFC1531.)

Option 78 specifies the location of one or more SLP Directory Agents. Option 79 specifies the list of scopes that a SLP Agent is configured to use.(RFC2610 - DHCP Options for Service Location Protocol)

Directory Agent (DA)

Diversity antenna and receiver

DNS

Domain Name Server

DSSS

Direct-Sequence Spread Spectrum. A transmission technology used in Local Area Wireless Network (LAWN) transmissions where a data signal at the sending station is combined with a higher data rate bit sequence, or chipping code, that divides the user data according to a spreading ratio. The chipping code is a redundant bit pattern for each bit that is transmitted, which increases the signal's resistance to interference. If one or more bits in the pattern are damaged during transmission, the original data can be recovered due to the redundancy of the transmission. (Compare FHSS)

DTIM

DTIM delivery traffic indication message (in 802.11 standard)

E

EAP-TLS
EAP-TTLS

EAP-TLS Extensible Authentication Protocol - Transport Layer Security. A general protocol for authentication that also supports multiple authentication methods, such as token cards, Kerberos, one-time passwords, certificates, public key authentication and smart cards. IEEE 802.1x specifies how EAP should be encapsulated in LAN frames.

In wireless communications using EAP, a user requests connection to a WLAN through an access point, which then requests the identity of the user and transmits that identity to an authentication server such as RADIUS. The server asks the access point for proof of identity, which the access point gets from the user and then sends back to the server to complete the authentication.

EAP-TLS provides for certificate-based and mutual authentication of the client and the network. It relies on client-side and server-side certificates to perform authentication and can be used to dynamically generate user-based and session-based WEP keys.

EAP-TTLS (Tunneled Transport Layer Security) is an extension of EAP-TLS to provide certificate-based, mutual authentication of the client and network through an encrypted tunnel, as well as to generate dynamic, per-user, per-session WEP keys. Unlike EAP-TLS, EAP-TTLS requires only server-side certificates.

(*See also* PEAP)

ELA (OPSEC)

Event Logging API (Application Program Interface) for OPSEC, a module in Check Point used to enable third-party applications to log events into the Check Point VPN-1/FireWall-1 management system.

Encapsulation

See tunnelling.

ESS

Extended Service Set (ESS). Several Basic Service Sets (BSSs) can be joined together to form one logical WLAN segment, referred to as an extended service set (ESS). The SSID is used to identify the ESS. (*See* BSS and SSID.)

F

FHSS

Frequency-Hopping Spread Spectrum. A transmission technology used in Local Area Wireless Network (LAWN) transmissions where the data signal is modulated with a narrowband carrier signal that "hops" in a random but predictable sequence from frequency to frequency as a function of time over a wide band of frequencies. This technique reduces interference. If synchronized properly, a single logical channel is maintained. (Compare DSSS)

F (Continued)

Fit, thin and fat APs

A thin AP architecture uses two components: an access point that is essentially a stripped-down radio and a centralized management controller that handles the other WLAN system functions. Wired network switches are also required.

A fit AP, a variation of the thin AP, handles the RF and encryption, while the central management controller, aware of the wireless users' identities and locations, handles secure roaming, quality of service, and user authentication. The central management controller also handles AP configuration and management.

A fat (or thick) AP architecture concentrates all the WLAN intelligence in the access point. The AP handles the radio frequency (RF) communication, as well as authenticating users, encrypting communications, secure roaming, WLAN management, and in some cases, network routing.

FQDN

Fully Qualified Domain Name. A “friendly” designation of a computer, of the general form computer.[subnetwork.].organization.domain. The FQDN names must be translated into an IP address in order for the resource to be found on a network, usually performed by a Domain Name Server.

FTM

Forwarding Table Manager

FTP

File Transfer Protocol

G

Gateway

In the wireless world, an access point with additional software capabilities such as providing NAT and DHCP. Gateways may also provide VPN support, roaming, firewalls, various levels of security, etc.

Gigabit Ethernet

The high data rate of the Ethernet standard, supporting data rates of 1 gigabit (1,000 megabits) per second.

GUI

Graphical User Interface

H

Heartbeat message

A heartbeat message is a UDP data packet used to monitor a data connection, polling to see if the connection is still alive.
In general terms, a heartbeat is a signal emitted at regular intervals by software to demonstrate that it is still alive. In networking, a heartbeat is the signal emitted by a Level 2 Ethernet transceiver at the end of every packet to show that the collision-detection circuit is still connected.

Host

(1) A computer (usually containing data) that is accessed by a user working on a remote terminal, connected by modems and telephone lines.

(2) A computer that is connected to a TCP/IP network, including the Internet. Each host has a unique IP address.

H (Continued)

HTTP Hypertext Transfer Protocol is the set of rules for transferring files (text, graphic images, sound, video, and other multimedia files) on the World Wide Web. A Web browser makes use of HTTP. HTTP is an application protocol that runs on top of the TCP/IP suite of protocols. (RFC2616: Hypertext Transfer Protocol -- HTTP/1.1)

HTTPS Hypertext Transfer Protocol over Secure Socket Layer, or HTTP over SSL, is a Web protocol that encrypts and decrypts user page requests as well as the pages that are returned by the Web server. HTTPS uses Secure Socket Layer (SSL) as a sublayer under its regular HTTP application layering. (HTTPS uses port 443 instead of HTTP port 80 in its interactions with the lower layer, TCP/IP.) SSL uses a 40-bit key size for the RC4 stream encryption algorithm, which is considered an adequate degree of encryption for commercial exchange.

I

IBSS Independent Basic Service Set. *See* BSS. An IBSS is the 802.11 term for an adhoc network. *See* adhoc network.

ICMP Internet Control Message Protocol, an extension to the Internet Protocol (IP) defined by RFC792. ICMP supports packets containing error, control, and informational messages. The PING command, for example, uses ICMP to test an Internet connection.

ICV ICV (Integrity Check Value) is a 4-byte code appended in standard WEP to the 802.11 message. Enhanced WPA inserts an 8-byte MIC just before the ICV. (*See* WPA and MIC)

IE Internet Explorer.

IEEE Institute of Electrical and Electronics Engineers, a technical professional association, involved in standards activities.

IETF Internet Engineering Task Force, the main standards organization for the Internet.

Infrastructure Mode An 802.11 networking framework in which devices communicate with each other by first going through an Access Point (AP). In infrastructure mode, wireless devices can communicate with each other or can communicate with a wired network. (*See* ad-hoc mode and BSS.)

Internet or IP telephony IP or Internet telephony are communications, such as voice, facsimile, voice-messaging applications, that are transported over the Internet, rather than the public switched telephone network (PSTN). IP telephony is the two-way transmission of audio over a packet-switched IP network (TCP/IP network).

An Internet telephone call has two steps: (1) converting the analog voice signal to digital format, (2) translating the signal into Internet protocol (IP) packets for transmission over the Internet. At the receiving end, the steps are reversed. Over the public Internet, voice quality varies considerably. Protocols that support Quality of Service (QoS) are being implemented to improve this.

I (Continued)

IP

Internet Protocol is the method or protocol by which data is sent from one computer to another on the Internet. Each computer (host) on the Internet has at least one IP address that uniquely identifies it. Internet Protocol specifies the format of packets, also called datagrams, and the addressing scheme. Most networks combine IP with a higher-level protocol called Transmission Control Protocol (TCP), which establishes a virtual connection between a destination and a source.

IPC

Interprocess Communication. A capability supported by some operating systems that allows one process to communicate with another process. The processes can be running on the same computer or on different computers connected through a network.

IPsec

Internet Protocol security (IPSec)

IPsec-ESP
IPsec-AH

Internet Protocol security Encapsulating Security Payload (IPsec-ESP). The encapsulating security payload (ESP) encapsulates its data, enabling it to protect data that follows in the datagram.Internet Protocol security Authentication Header (IPsec-AH). AH protects the parts of the IP datagram that can be predicted by the sender as it will be received by the receiver.IPsec is a set of protocols developed by the IETF to support secure exchange of packets at the IP layer. IPsec has been deployed widely to implement Virtual Private Networks (VPNs). IPsec supports two encryption modes: Transport and Tunnel. Transport mode encrypts only the data portion (payload) of each packet, but leaves the header untouched. The more secure Tunnel mode encrypts both the header and the payload. On the receiving side, an IPSec-compliant device decrypts each packet. For IPsec to work, the sending and receiving devices must share a public key. This is accomplished through a protocol known as Internet Security Association and Key Management Protocol/Oakley (ISAKMP/Oakley), which allows the receiver to obtain a public key and authenticate the sender using digital certificates.

isochronous

Isochronous data is data (such as voice or video) that requires a constant transmission rate, where data must be delivered within certain time constraints. For example, multimedia streams require an isochronous transport mechanism to ensure that data is delivered as fast as it is displayed and to ensure that the audio is synchronized with the video. Compare: asynchronous processes in which data streams can be broken by random intervals, and synchronous processes, in which data streams can be delivered only at specific intervals.

ISP

Internet Service Provider.

IV

IV (Initialization Vector), part of the standard WEP encryption mechanism that concatenates a shared secret key with a randomly generated 24-bit initialization vector. WPA with TKIP uses 48-bit IVs, an enhancement that significantly increases the difficulty in cracking the encryption. (*See* WPA and TKIP)

L

LAN — Local Area Network.

LSA — Link State Advertisements received by the currently running OSPF process. The LSAs describe the local state of a router or network, including the state of the router's interfaces and adjacencies. *See* also OSPF.

M

MAC — Media Access Control layer. One of two sublayers that make up the Data Link Layer of the OSI model. The MAC layer is responsible for moving data packets to and from one Network Interface Card (NIC) to another across a shared channel.

MAC address — Media Access Control address. A hardware address that uniquely identifies each node of a network.

MIB — Management Information Base is a formal description of a set of network objects that can be managed using the Simple Network Management Protocol (SNMP). The format of the MIB is defined as part of the SNMP. A MIB is a collection of definitions defining the properties of a managed object within a device. Every managed device keeps a database of values for each of the definitions written in the MIB. Definition of the MIB conforms to RFC1155 (Structure of Management Information).

MIC — Message Integrity Check or Code (MIC), also called “Michael”, is part of WPA and TKIP. The MIC is an additional 8-byte code inserted before the standard 4-byte integrity check value (ICV) that is appended in by standard WEP to the 802.11 message. This greatly increases the difficulty in carrying out forgery attacks.

Both integrity check mechanisms are calculated by the receiver and compared against the values sent by the sender in the frame. If the values match, there is assurance that the message has not been tampered with. (*See* WPA, TKIP and ICV).

MTU — Maximum Transmission Unit. The largest packet size, measured in bytes, that a network interface is configured to accept. Any messages larger than the MTU are divided into smaller packets before being sent.

MU — Mobile Unit, a wireless device such as a PC laptop.

multicast, broadcast, unicast — Multicast: transmitting a single message to a select group of recipients. Broadcast: sending a message to everyone connected to a network. Unicast: communication over a network between a single sender and a single receiver.

N

NAS Network Access Server, a server responsible for passing information to designated RADIUS Servers and then acting on the response returned. A NAS-Identifier is a RADIUS attribute identifying the NAS server. (RFC2138)

NAT Network Address Translator. A network capability that enables a group of computers to dynamically share a single incoming IP address. NAT takes the single incoming IP address and creates new IP address for each client computer on the network.

Netmask In administering Internet sites, a netmask is a string of 0's and 1's that mask or screen out the network part of an IP address, so that only the host computer part of the address remains. A frequently-used netmask is 255.255.255.0, used for a Class C subnet (one with up to 255 host computers). The ".0" in the "255.255.255.0" netmask allows the specific host computer address to be visible.

NIC Network Interface Card. An expansion board in a computer that connects the computer to a network.

NMS Network Management System. The system responsible for managing a network or a portion of a network. The NMS talks to network management agents, which reside in the managed nodes.

NTP Network Time Protocol, an Internet standard protocol (built on top of TCP/IP) that assures accurate synchronization to the millisecond of computer clock times in a network of computers. Based on UTC, NTP synchronizes client workstation clocks to the U.S. Naval Observatory Master Clocks in Washington, DC and Colorado Springs CO. Running as a continuous background client program on a computer, NTP sends periodic time requests to servers, obtaining server time stamps and using them to adjust the client's clock. (RFC1305)

O

OFDM Orthogonal frequency division multiplexing, a method of digital modulation in which a signal is split into several narrowband channels at different frequencies. OFDM is similar to conventional frequency division multiplexing (FDM). The difference lies in the way in which the signals are modulated and demodulated. Priority is given to minimizing the interference, or crosstalk, among the channels and symbols comprising the data stream. Less importance is placed on perfecting individual channels.

OFDM is used in European digital audio broadcast services. It is also used in wireless local area networks.

OID Object Identifier.

OPSEC OPSEC (Open Platform for Security) is a security alliance program created by Check Point to enable an open industry-wide framework for interoperability of security products and applications. Products carrying the "Secured by Check Point" seal have been tested to guarantee integration and interoperability.

O (Continued)

OS
Operating system.

OSI
Open System Interconnection. An ISO standard for worldwide communications that defines a networking framework for implementing protocols in seven layers. Control is passed from one layer to the next, starting at the application layer in one station, down through the presentation, session, transport, network, data link layer to the physical layer at the bottom, over the channel to the next station and back up the hierarchy.

OSI Layer 2
At the Data Link layer (OSI Layer 2), data packets are encoded and decoded into bits. The data link layer has two sublayers:

- the Logical Link Control (LLC) layer controls frame synchronization, flow control and error checking
- The Media Access Control (MAC) layer controls how a computer on the network gains access to the data and permission to transmit it.

OSI Layer 3
The Network layer (OSI Layer 3) provides switching and routing technologies, creating logical paths, known as virtual circuits, for transmitting data from node to node. Routing and forwarding are functions of this layer, as well as addressing, internetworking, error handling, congestion control and packet sequencing.

OSPF
Open Shortest Path First, an interior gateway routing protocol developed for IP networks based on the shortest path first or link-state algorithm. Routers use link-state algorithms to send routing information to all nodes in an internetwork by calculating the shortest path to each node based on a topography of the Internet constructed by each node. Each router sends that portion of the routing table (keeps track of routes to particular network destinations) that describes the state of its own links, and it also sends the complete routing structure (topography). Using OSPF, a host that obtains a change to a routing table or detects a change in the network immediately multicasts the information to all other hosts in the network so that all will have the same routing table information. The host using OSPF sends only the part that has changed, and only when a change has taken place. (RFC2328)

OUI
Organizationally Unique Identifier (used in MAC addressing).

P

Packet
The unit of data that is routed between an origin and a destination on the Internet or any other packet-switched network. When any file is sent from one place to another on the Internet, the Transmission Control Protocol (TCP) layer of TCP/IP divides the file into packets. Each packet is separately numbered and includes the Internet address of the destination. The individual packets for a given file may travel different routes through the Internet. When they have all arrived, they are reassembled into the original file (by the TCP layer at the receiving end).

P (Continued)

PAP — Password Authentication Protocol is the most basic form of authentication, in which a user's name and password are transmitted over a network and compared to a table of name-password pairs. Typically, the passwords stored in the table are encrypted. (*See* CHAP).

PDU — Protocol Data Unit. A data object exchanged by protocol machines (such as management stations, SMUX peers, and SNMP agents) and consisting of both protocol control information and user data. PDU is sometimes used as a synonym for “packet''.

PEAP — PEAP (Protected Extensible Authentication Protocol) is an IETF draft standard to authenticate wireless LAN clients without requiring them to have certificates. In PEAP authentication, first the user authenticates the authentication server, then the authentication server authenticates the user. If the first phase is successful, the user is then authenticated over the SSL tunnel created in phase one using EAP-Generic Token Card (EAP-GTC) or Microsoft Challenged Handshake Protocol Version 2 (MSCHAP V2). (*See* also EAP-TLS).

PHP server — Hypertext Preprocessor

PKI — Public Key Infrastructure

PoE — Power over Ethernet. The Power over Ethernet standard (802.3af) defines how power can be provided to network devices over existing Ethernet connection, eliminating the need for additional external power supplies.

POST — Power On Self Test, a diagnostic testing sequence performed by a computer to determine if its hardware elements are present and powered on. If so, the computer begins its boot sequence.

push-to-talk (PTT) — The push-to-talk (PTT) is feature on wireless telephones that allows them to operate like a walkie-talkie in a group, instead of standard telephone operation. The PTT feature requires that the network be configured to allow multicast traffic.

A PTT call is initiated by selecting a channel and pressing the “talk” key on the wireless telephone. All wireless telephones on the same network that are monitoring the channel will hear the transmission. On a PTT call you hold the button to talk and release it to listen.

Q

QoS — Quality of Service. A term for a number of techniques that intelligently match the needs of specific applications to the network resources available, using such technologies as Frame Relay, Asynchronous Transfer Mode (ATM), Ethernet and 802.1 networks, SONET, and IP-routed networks. QoS features provide better network service by supporting dedicated bandwidth, improving loss characteristics, avoiding and managing network congestion, shaping network traffic, setting traffic priorities across the network.

Quality-of-Service (QoS): A set of service requirements to be met by the network while transporting a flow. (RFC2386)

R

RADIUS Remote Authentication Dial-In User Service. An authentication and accounting system that checks User Name and Password and authorizes access to a network. The RADIUS specification is maintained by a working group of the IETF (RFC2865 RADIUS, RFC2866 RADIUS Accounting, RFC2868 RADIUS Attributes for Tunnel Protocol Support).

RF Radio Frequency, a frequency in the electromagnetic spectrum associated with radio wave propagation. When an RF current is supplied to an antenna, an electromagnetic field is created that can propagate through space. These frequencies in the electromagnetic spectrum range from Ultra-low frequency (ULF) -- 0-3 Hz to Extremely high frequency (EHF) -- 30GHz - 300 GHz. The middle ranges are: Low frequency (LF) -- 30 kHz - 300 kHz, Medium frequency (MF) -- 300 kHz - 3 MHz, High frequency (HF) -- 3MHz - 30 MHz, Very high frequency (VHF) -- 30 MHz - 300 MHz, Ultra-high frequency (UHF)-- 300MHz - 3 GHz.

RFC Request for Comments, a series of notes about the Internet, submitted to the Internet Engineering Task Force (IETF) and designated by an RFC number, that may evolve into an Internet standard. The RFCs are catalogued and maintained on the IETF RFC website: www.ietf.org/rfc.html.

Roaming In 802.11, roaming occurs when a wireless device (a station) moves from one Access Point to another (or BSS to another) in the same Extended Service Set (ESS) -identified by its SSID.

RP-SMA Reverse Polarity-Subminiature version A, a type of connector used with wireless antennas

RSN Robust Security Network. A new standard within IEEE 802.11 to provide security and privacy mechanisms. The RSN (and related TSN) both specify IEEE 802.1x authentication with Extensible Authentication Protocol (EAP).

RSSI RSSI received signal strength indication (in 802.11 standard)

RTS / CTS RTS request to send, CTS clear to send (in 802.11 standard)

S

Segment

In ethernet networks, a section of a network that is bounded by bridges, routers or switches. Dividing a LAN segment into multiple smaller segments is one of the most common ways of increasing available bandwidth on the LAN.

SLP

Service Location Protocol. A method of organizing and locating the resources (such as printers, disk drives, databases, e-mail directories, and schedulers) in a network. Using SLP, networking applications can discover the existence, location and configuration of networked devices.

With Service Location Protocol, client applications are 'User Agents' and services are advertised by 'Service Agents'. The User Agent issues a multicast 'Service Request' (SrvRqst) on behalf of the client application, specifying the services required. The User Agent will receive a Service Reply (SrvRply) specifying the location of all services in the network which satisfy the request.

For larger networks, a third entity, called a 'Directory Agent', receives registrations from all available Service Agents. A User Agent sends a unicast request for services to a Directory Agent (if there is one) rather than to a Service Agent.

(SLP version 2, RFC2608, updating RFC2165)

SMI

Structure of Management Information. A hierarchical tree structure for information that underlies Management Information Bases (MIBs), and is used by the SNMP protocol. Defined in RFC1155 and RFC1442 (SNMPv2).

SMT (802.11)

Station ManagemenT. The object class in the 802.11 MIB that provides the necessary support at the station to manage the processes in the station such that the station may work cooperatively as a part of an IEEE 802.11 network. The four branches of the 802.11 MIB are:

- dot11smt - objects related to station management and local configuration
- dot11mac - objects that report/configure on the status of various MAC parameters
- dot11res - Objects that describe available resources
- dot11phy - Objects that report on various physical items.

SNMP

Simple Network Management Protocol. A set of protocols for managing complex networks. SNMP works by sending messages, called protocol data units (PDUs), to different parts of a network. SNMP-compliant devices, called agents, store data about themselves in Management Information Bases (MIBs) and return this data to the SNMP requesters.

SNMP includes a limited set of management commands and responses. The management system issues Get, GetNext and Set messages to retrieve single or multiple object variables or to establish the value of a single variable. The managed agent sends a Response message to complete the Get, GetNext or Set.

S (Continued)

SNMP trap

An event notification sent by the SNMP managed agent to the management system to identify the occurrence of conditions (such as a threshold that exceeds a predetermined value).

SSH

Secure Shell, sometimes known as Secure Socket Shell, is a Unix-based command interface and protocol for securely getting access to a remote computer. SSH is a suite of three utilities - slogin, ssh, and scp - secure versions of the earlier UNIX utilities, rlogin, rsh, and rcp. With SSH commands, both ends of the client/server connection are authenticated using a digital certificate, and passwords are protected by being encrypted.

SSID

Service Set Identifier. A 32-character unique identifier attached to the header of packets sent over a Wireless LAN that acts as a password when a wireless device tries to connect to the Basic Service Set (BSS). Several BSSs can be joined together to form one logical WLAN segment, referred to as an extended service set (ESS). The SSID is used to identify the ESS.

In 802.11 networks, each Access Point advertises its presence several times per second by broadcasting beacon frames that carry the ESS name (SSID). Stations discover APs by listening for beacons, or by sending probe frames to search for an AP with a desired SSID. When the station locates an appropriately-named Access Point, it sends an associate request frame containing the desired SSID. The AP replies with an associate response frame, also containing the SSID.

Some APs can be configured to send a zero-length broadcast SSID in beacon frames instead of sending their actual SSID. The AP must return its actual SSID in the probe response.

SSL

Secure Sockets Layer. A protocol developed by Netscape for transmitting private documents via the Internet. SSL works by using a public key to encrypt data that's transferred over the SSL connection. URL's that require an SSL connection start with https: instead of http.

SSL uses a program layer located between the Internet's Hypertext Transfer Protocol (HTTP) and Transport Control Protocol (TCP) layers. The “sockets” part of the term refers to the sockets method of passing data back and forth between a client and a server program in a network or between program layers in the same computer. SSL uses the public-and-private key encryption system from RSA, which also includes the use of a digital certificate.

SSL has recently been succeeded by Transport Layer Security (TLS), which is based on SSL.

Subnet mask

(*See* netmask)

Subnets

Portions of networks that share the same common address format. A subnet in a TCP/IP network uses the same first three sets of numbers (such as 198.63.45.xxx), leaving the fourth set to identify devices on the subnet. A subnet can be used to increase the bandwidth on the network by breaking the network up into segments.

S (Continued)

SVP

SpectraLink Voice Protocol, a protocol developed by SpectraLink to be implemented on access points in order to facilitate voice prioritization over an 802.11 wireless LAN that will carry voice packets from SpectraLink wireless telephones.

Switch

In networks, a device that filters and forwards packets between LAN segments. Switches operate at the data link layer (layer 2) and sometimes the network layer (layer 3) of the OSI Reference Model and therefore support any packet protocol. LANs that use switches to join segments are called switched LANs or, in the case of Ethernet networks, switched Ethernet LANs.

syslog

A protocol used for the transmission of event notification messages across networks, originally developed on the University of California Berkeley Software Distribution (BSD) TCP/IP system implementations, and now embedded in many other operating systems and networked devices. A device generates a messages, a relay receives and forwards the messages, and a collector (a syslog server) receives the messages without relaying them.

Syslog uses the user datagram protocol (UDP) as its underlying transport layer mechanism. The UDP port that has been assigned to syslog is 514. (RFC3164)

T

TCP / IP

Transmission Control Protocol. TCP, together with IP (Internet Protocol), is the basic communication language or protocol of the Internet. Transmission Control Protocol manages the assembling of a message or file into smaller packets that are transmitted over the Internet and received by a TCP layer that reassembles the packets into the original message. Internet Protocol handles the address part of each packet so that it gets to the right destination.

TCP/IP uses the client/server model of communication in which a computer user (a client) requests and is provided a service (such as sending a Web page) by another computer (a server) in the network.

TFTP

Trivial File Transfer Protocol. An Internet software utility for transferring files that is simpler to use than the File Transfer Protocol (FTP) but less capable. It is used where user authentication and directory visibility are not required. TFTP uses the User Datagram Protocol (UDP) rather than the Transmission Control Protocol (TCP). TFTP is described formally in Request for Comments (RFC) 1350.

TKIP

Temporal Key Integrity Protocol (TKIP) is an enhancement to the WEP encryption technique that uses a set of algorithms that rotates the session keys. TKIP's enhanced encryption includes a per-packet key mixing function, a message integrity check (MIC), an extended initialization vector (IV) with sequencing rules, and a re-keying mechanism. The encryption keys are changed (rekeyed) automatically and authenticated between devices after the rekey interval (either a specified period of time, or after a specified number of packets has been transmitted).

T (Continued)

TLS

Transport Layer Security. (*See* EAP, Extensible Authentication Protocol)

ToS / DSCP

ToS (Type of Service) / DSCP (Diffserv Codepoint). The ToS/DSCP field contained in the IP header of a frame is used by applications to indicate the priority and Quality of Service (QoS) for each frame. The level of service is determined by a set of service parameters which provide a three way trade-off between low-delay, high-reliability, and high-throughput. The use of service parameters may increase the cost of service.

TSN

Transition Security Network. A subset of Robust Security Network (RSN), which provides an enhanced security solution for legacy hardware. The Wi-Fi Alliance has adopted a solution called Wireless Protected Access (WPA), based on TSN. RSN and TSN both specify IEEE 802.1x authentication with Extensible Authentication Protocol (EAP).

Tunnelling

Tunnelling (or encapsulation) is a technology that enables one network to send its data via another network's connections. Tunnelling works by encapsulating packets of a network protocol within packets carried by the second network. The receiving device then decapsulates the packets and forwards them in their original format.

U

UDP

User Datagram Protocol. A connectionless protocol that, like TCP, runs on top of IP networks. Unlike TCP/IP, UDP/IP provides very few error recovery services, offering instead a direct way to send and receive packets over an IP network. It is used primarily for broadcasting messages over a network.

U-NII

Unlicensed National Information Infrastructure. Designated to provide short-range, high-speed wireless networking communication at low cost, U-NII consists of three frequency bands of 100 MHz each in the 5 GHz band: 5.15-5.25GHz (for indoor use only), 5.25-5.35 GHz and 5.725-5.825GHz. The three frequency bands were set aside by the FCC in 1997 initially to help schools connect to the Internet without the need for hard wiring. U-NII devices do not require licensing.

URL

Uniform Resource Locator. the unique global address of resources or files on the World Wide Web. The URL contains the name of the protocol to be used to access the file resource, the IP address or the domain name of the computer where the resource is located, and a pathname -- a hierarchical description that specifies the location of a file in that computer.

V

VLAN

Virtual Local Area Network. A network of computers that behave as if they are connected to the same wire when they may be physically located on different segments of a LAN. VLANs are configured through software rather than hardware, which makes them extremely flexible. When a computer is physically moved to another location, it can stay on the same VLAN without any hardware reconfiguration.

The standard is defined in IEEE 802.1Q - Virtual LANs, which states that "IEEE 802 Local Area Networks (LANs) of all types may be connected together with Media Access Control (MAC) Bridges, as specified in ISO/IEC 15802-3. This standard defines the operation of Virtual LAN (VLAN) Bridges that permit the definition, operation and administration of Virtual LAN topologies within a Bridged LAN infrastructure."

WM-AD

WM Access Domain Services (WM-AD). An Extreme Networks-specific technique that provides a means of mapping wireless networks to a wired topology.

VoIP

Voice Over Internet Protocol. An internet telephony technique. With VoIP, a voice transmission is cut into multiple packets, takes the most efficient path along the Internet and is reassembled when it reaches the destination.

VPN

Virtual Private Network. A private network that is constructed by using public wires to connect nodes. These systems use encryption and other security mechanisms to ensure that only authorized users can access the network and that the data cannot be intercepted.

VSA

Vendor Specific Attribute, an attribute for a RADIUS server defined by the manufacturer.(compared to the RADIUS attributes defined in the original RADIUS protocol RFC2865). A VSA attribute is defined in order that it can be returned from the RADIUS server in the Access Granted packet to the Radius Client.

W

Walled Garden

A restricted subset of network content that wireless devices can access.

WEP

Wired Equivalent Privacy. A security protocol for wireless local area networks (WLANs) defined in the 802.11b standard. WEP aims to provide security by encrypting data over radio waves so that it is protected as it is transmitted from one end point to another.

Wi-Fi

Wireless fidelity. A term referring to any type of 802.11 network, whether 802.11b, 802.11a, dual-band, etc. Used in reference to the Wi-Fi Alliance, a nonprofit international association formed in 1999 to certify interoperability of wireless Local Area Network products based on IEEE 802.11 specification.

W (Continued)

WINS

Windows Internet Naming Service. A system that determines the IP address associated with a particular network computer, called name resolution. WINS supports network client and server computers running Windows and can provide name resolution for other computers with special arrangements. WINS supports dynamic addressing (DHCP) by maintaining a distributed database that is automatically updated with the names of computers currently available and the IP address assigned to each one.

DNS is an alternative system for name resolution suitable for network computers with fixed IP addresses.

WLAN

Wireless Local Area Network.

WMM

Wi-Fi Multimedia (WMM), a Wi-Fi Alliance certified standard that provides multimedia enhancements for Wi-Fi networks that improve the user experience for audio, video, and voice applications. This standard is complicant with the IEEE 802.11e Quality of Service (QoS) extensions for 802.11 networks. WMM provides prioritized media access by shortening the time between transmitting packets for higher priority traffic. WMM is based on the Enhanced Distributed Channel Access (EDCA) method.

WPA

Wireless Protected Access, or Wi-Fi Protected Access is a security solution adopted by the Wi-Fi Alliance that adds authentication to WEP's basic encryption. For authentication, WPA specifies IEEE 802.1x authentication with Extensible Authentication Protocol (EAP). For encryption, WPA uses the Temporal Key Integrity Protocol (TKIP) mechanism, which shares a starting key between devices, and then changes their encryption key for every packet. Certificate Authentication (CA) can also be used. Also part of the encryption mechanism are 802.1X for dynamic key distribution and Message Integrity Check (MIC) a.k.a. “Michael”.

WPA requires that all computers and devices have WPA software.

WPA-PSK

Wi-Fi Protected Access with Pre-Shared Key, a special mode of WPA for users without an enterprise authentication server. Instead, for authentication, a Pre-Shared Key is used. The PSK is a shared secret (passphrase) that must be entered in both the Altitude Access Point or router and the WPA clients.

This preshared key should be a random sequence of characters at least 20 characters long or hexadecimal digits (numbers 0-9 and letters A-F) at least 24 hexadecimal digits long. After the initial shared secret, the Temporal Key Integrity Protocol (TKIP) handles the encryption and automatic rekeying.

Summit WM-Series Switch Software terms and abbreviations

Term	Explanation
CTP	CAPWAP Tunnelling Protocol (CTP). The Altitude AP uses a UDP (User Datagram Protocol) based tunnelling protocol called CAPWAP Tunnelling Protocol (CTP) to encapsulate the 802.11 packets and forward them to the Summit WM-Series Switch. The CTP protocol defines a mechanism for the control and provisioning of wireless access points (CAPWAP) through centralized access controllers. In addition, it provides a mechanism providing the option to tunnel the mobile client data between the access point and the access controller.
Auto Cell	The Auto Cell feature consists of software on the Altitude AP that provides dynamic radio frequency (RF) management. For Altitude APs with the Auto Cell feature enabled and on a common channel, the power levels will be adjusted to balance coverage if a Altitude AP is added to, or leaves, the network. The feature also allows wireless clients to be moved to another Altitude AP if the load is too high. The feature can also be set to scan automatically for a channel, using a channel selection algorithm.
Summit WM-Series Switch	The Summit WM-Series Switch is a rack-mountable network device designed to be integrated into an existing wired Local Area Network (LAN). It provides centralized control over all access points (both Altitude APs and third-party access points) and manages the network assignment of wireless device clients associating through access points.
Langley	"Langley" is a Summit WM-Series Switch Software term for the inter-process messaging infrastructure on the Summit WM-Series Switch.
Summit Spy	The Summit Spy is a mechanism that assists in the detection of rogue access points. The feature has three components: (1) a radio frequency (RF) scanning task that runs on the Altitude AP, (2) an application called the RF Data Collector (RFDC) on the Summit WM-Series Switch that receives and manages the RF scan messages sent by the Altitude AP, (3) an Analysis Engine on the Summit WM-Series Switch that processes the scan data.
RFDC	The RF Data Collector (RFDC) is an application on the Summit WM-Series Switch that receives and manages the Radio Frequency (RF) scan messages sent by the Altitude AP. This application is part of the Summit Spy technique, working in conjunction with the scanner mechanism and the analysis engine to assist in detecting rogue access points.
WM Access Domain Services (WM-AD)	The WM Access Domain Services (WM-AD) technique is the Extreme Networks means of mapping wireless networks to the topology of an existing wired network. When you set up WM Access Domain Services (WM-AD) on the Summit WM-Series Switch, you are defining subnets for groups of wireless users. This WM-AD definition creates a virtual IP subnet where the Summit WM-Series Switch acts as a default gateway for wireless devices. This technique enables policies and authentication to be applied to the groups of wireless users on a WM-AD, as well as the collecting of accounting information. When a WM-AD is set up on the Summit WM-Series Switch, one or more Altitude APs (by radio) are associated with it. A range of IP addresses is set aside for the Summit WM-Series Switch's DHCP server to assign to wireless devices.

Term	Explanation
WM-AD Manager (and WM-AD Agent)	The technique in Summit WM-Series Switch Software by which multiple Summit WM-Series Switches on a network can discover each other and exchange information about a client session. This enables a wireless device user to roam seamlessly between different Altitude APs on different Summit WM-Series Switches, to provide mobility to the wireless device user. One Summit WM-Series Switch on the network must be designated as the "WM-AD Manager". All other Summit WM-Series Switches are designated as "WM-AD Agents". Relying on SLP, the WM-AD Manager registers with the Directory Agent and the WM-AD Agents discover the location of the WM-AD Manager.
Altitude AP	The Altitude AP is a wireless LAN thin access point (IEEE 802.11) provided with unique software that allows it to communicate only with a Summit WM-Series Switch. (A thin access point handles the radio frequency (RF) communication but relies on a controller to handle WLAN elements such as authentication.) The Altitude AP also provides local processing such as encryption. The Altitude AP is a dual-band access point, with both 802.11a and 802.11b/g radios.

A Summit WM-Series Switch Software system states and LEDs

Summit WM-Series Switch system states and LEDs

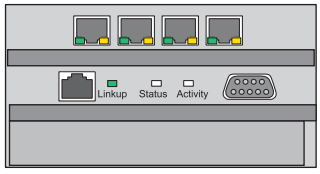
The Summit WM-Series Switch has the two system states: Standby and Active.

It enters "Standby" when shut down in the *Summit WM-Series Switch Configuration – System Maintenance* screen. The Summit WM-Series Switch:

- sends control message to Altitude AP to enter "Standby" state
- will not handle any wireless traffic or sessions
- disables DHCP, Policy Manager, Security Manager, Altitude AP Manager, Redirector
- remains on the wired network

It enters "Active" state on startup in the user interface. The Summit WM-Series Switch can now respond to the Altitude AP's "discover" message by returning a message that the Altitude AP can enter the "active" state.

The activity and traffic on the Summit WM-Series Switch can be monitored via three LEDs on the back of the Summit WM-Series Switch: Link, Status, Activity.



The three LEDs perform the following functions:

- Link LED: Displays the link status of management port Ethernet link as seen by the system software.
- Status LED: Indicates the state of the CM from software point of view, normal operation, whether processes have gone down and are restarting, etc.
- Activity LED: Indicates the amount of traffic carried to and from Altitude APs.

The Link LED is only seen at the back of the Summit WM-Series Switch. The Status and Activity LEDs can be seen from both the front and the back of the Summit WM-Series Switch.

The sequence of the Status and Activity LEDs is as follows:

System State	Status LED	Activity LED
Power up	Off	Off
Services started: WDTSTAT installed (init.d starts services)	Blinking Amber	Off
Startup Manager Task started	Solid Amber	Blinking Amber
Startup Manager Task completes startup – all components started	Solid Green	Blinking green, if traffic Blank, if no traffic

System State	Status LED	Activity LED
A component fails to start or needs restarting (Startup Manager Task retrying that component)	Solid Amber	Blinking green
Summit WM-Series Switch fails to boot	Solid Red	Off
A component fails (no more retries)	Solid Red	Off
System about to be reset by watchdog	Blinking Red	Off

Altitude AP system states

For the Altitude AP the Status LED in the center also indicates power. The Status LED is dark when unit is off and is green (solid) when the AP has completed discovery and is operational.

The chart below shows states and corresponding Status LED displays:

Table 6: Altitude AP system states and status LED displays

State / Process	Description	LEDs
Power	Altitude AP not powered.	Off
Power	Start up: Power On Self Test (POST)	Steady green (briefly)
Power	Power On Self Test (POST) successful	Off (briefly)
Discovery	If the POST self test is successful, the AP begins “Discovery” process. Altitude AP is powered on and searching for an active Summit WM-Series Switch. It sends a “discover” message and waits for a response	Orange (steady)
Fail to find DHCP	Altitude AP failed to find DHCP (will stay in this state until a route appears).	Red-orange (alternate blink)
Failed discovery	If there are SLP issues in failed discovery, the LED display changes.	Green-orange (alternate blink)
Registration	Altitude AP learns the Summit WM-Series Switch's IP address, and can begin the Registration process	Orange (blink)
Failed Registration	Altitude AP fails to learn the Summit WM-Series Switch's IP address.	Red (blink)
Standby	1. Altitude AP enters this state from “Discovery” when it encounters an active Summit WM-Series Switch and completes the Registration process.	Green (blink)
	2. Altitude AP enters this state from “Active” when it receives a control message from the Summit WM-Series Switch to enter this state. If the Altitude AP has any wireless device traffic, it will drop the traffic.	
	Altitude AP fails to register. It will wait 5 seconds and try again.	Red (slow blink)
	Firmware download from the Summit WM-Series Switch is in progress	Orange + green (blink)
Active (Ready)	Altitude AP has received a control message from an active Summit WM-Series Switch to enter “active” or “ready” state. It is ready to receive wireless traffic.	Green (steady)
	Note: The two Traffic LEDs on either side of the Status LED display a green (blink) if there is active wireless traffic. The left LED is for the 2.4 GHz radio. The right LED is for the 5 GHz radio.	

B CLI command reference

Table 7: CLI commands

Category		Syntax	Comment
Top Level	<hostname>#	ip	
		interface	
		exit	quit ssh session
		logout	logs out of system
System State	<hostname>#	shutdown <rebootlhalt>	requires confirmation
	<hostname>#	reset <database>	requires confirmation
	<hostname>#	reset <factory>	requires confirmation
System Maintenance			
	<hostname>#	loglevel <1l2l3l4l5>	
	<hostname>#	syslog	
	<hostname>:syslog#	syslogip # <xxx.xxx.xxx.xxx>	
	<hostname>:syslog#	(no) syslog #	
	<hostname>:syslog#	(no) svcmsg	
	<hostname>:syslog#	logs <hostname> #	(0,1,3,4,5,6: valid numbers;default is 0)
	<hostname>:syslog#	logs service #	(0,1,3,4,5,6: valid numbers; default is 3)
	<hostname>:syslog#	logs application #	(0,1,3,4,5,6: valid numbers; default is 3)
	<hostname>#	show loglevel=<critical l major l minor l info>	output log to console
Routing Protocols			
Static Routes	<hostname>#	ip	
	<hostname>:ip#	route <address/mask> <x.y.z.a> <onloff>	creates a static route
	OR	route <address> <mask> <x.y.z.a> <onloff>	alternate format
	<hostname>:ip#	route <a.b.c.d> <onloff>	creates default route; ip keyword optional
	<hostname>:ip#	show routes	displays a numbered table of static routes
	<hostname>:ip#	no route #n	clears static route #n
	OR	no route <x.y.z.a>	clears static route; has to match an existing route with address x.y.z.a

Table 7: CLI commands (Continued)

Category		Syntax	Comment
OSPF	<hostname>#	ip	
	<hostname>:ip#	(no) protocol ospf	
	<hostname>:ip#	ospf	only 1 protocol can be enabled on the AC
	<hostname>:ospf#	routerid <value>	
		area <area-id>	
		areatype <default|stub|nssa>	
		config ospfinterface <0|1|2|3>	
	<hostname>:ospf.0#	(no) ospfinterface	Port has to be made router port during esa configuration
		linkcost <valldefault>	
		auth <on|off>	
		authkey <password>	
		hello <valldefault>	
		dead <valldefault>	
		retx <valldefault>	
		txdelay <valldefault>	
IP Addresses			
Management Port	<hostname>#	interface	
	<hostname>:interface:#	eth0	selects interface to configure
	<hostname>:interface: eth0#	hostname '<string>'	hostname
	<hostname>:interface: eth0#	domain '<string>'	domain name
	<hostname>:interface :eth0#	ip <xxx.xxx.xxx.xxx>/mask	enter management IP address
	OR	ip <xxx.xxx.xxx.xxx> mask <255.255.255.255>	enter network mask
	<hostname>:interface: eth0#	gateway <xxx.xxx.xxx.xxx>	enter gateway address
	<hostname>:interface: eth0#	(no) nameserver # <x.y.z.a>	(opt) domain controller addresses
		exit	return to <hostname>(if)#
esa Ports	<hostname>:interface:#	esa [0-3]	
	<hostname>:interface: esa-X#	ip <xxx.xxx.xxx.xxx>/mask	enter IXP port IP address
	OR	ip <xxx.xxx.xxx.xxx> mask <255.255.255.255>	enter network mask
	<hostname>:interface: esa-X#	#mtu <integer>	has to be 64 <= X <= 1500
	<hostname>:interface: esa-X#	function [host | ap | router]	set interface type
	<hostname>:interface: esa-X#	(no) mgmt	enable / disable management traffic
	<hostname>:interface: esa-X#	(no) regslp	register interface with slp

Table 7: CLI commands (Continued)

Category		Syntax	Comment
File Management			
	<hostname>#	show backup [filenamelnumber]	list back-up files on system
	<hostname>#	show cdrs [dir] [filenamelnumber]	list CDRs available on system
	<hostname>#	show restore	list restore files on system
	<hostname>#	show upgrade	list upgrade files on system
	<hostname>#	show osupgrade	list os upgrade files on system
	<hostname>#	show apup	list ap image upgrade files on system
	<hostname>#	show bootrom	list ap bootrom image files on system
Back-up system	<hostname>#	backup <cdrslconfigurationllogslauditlall>	
Restore Back-up	<hostname>#	restore <filenamelnumber>	
Upgrade CM	<hostname>#	upgrade ac <filenamelnumber>	
Upgrade OS	<hostname>#	upgrade os <filenamelnumber>	
Upgrade AP	<hostname>#	upgrade apup <filenamelnumber> ap <bserial#, ..., bserial#>	
Upgrade Product Key	<hostname>#	upgrade key	executes script to apply product key
Upload / Download	<hostname>#	copy backup <server> <user> <dir> <file>	
		copy restore <server> <user> <dir> <file>	
		copy upgrade <server> <user> <dir> <file>	
		copy osupgrade <server> <user> <dir> <file>	
		copy cdrs <server> <user> <dir> <file>	
		copy apup <server> <user> <dir> <file>	
		copy key <server> <user><dir> <file>	loads key onto server
		no backup <filenamelnumber>	deletes backup file
		no restore <filenamelnumber>	deletes restore file
		no upgrade <filenamelnumber>	deletes upgrade file
		no apup <filenamelnumber>	deletes ap upgrade image
		no cdr <filenamelnumber>	deletes cdr record
		no key	deletes key – only available from the CLI

Table 7: CLI commands (Continued)

Category		Syntax	Comment
Users	<hostname>#	users	
	<hostname>:users#id	<userid> [admin] [enableldisable]	end of command, enter password & confirm password
	<hostname>:users#id	no id <userid>	confirm delete
	<hostname>:users#id	(no) logon <userid>	disable / enable user access to management system; confirm action
	<hostname>:users#id	pwd id <userid>	change password for userid; enter password & confirm password
Diagnostics	<hostname>#	ping <target_ip>	issues 4 iCMP ping messages to target IP address
	<hostname>#	traceroute <target_ip>	attempts to trace route to target IP address
		radtest <wm-ad_name> <username> <password>][tracing]	tests RADIUS authentication settings
		radtest_mba <wm-ad> <mac> <ap_bss_mac> <ap_eth_mac> [tracing]	tests RADIUS MAC-based authentication
Altitude APs	<hostname>#	show ap	displays list of AP serial numbers

C DHCP, SLP, and Option 78 reference

For the Altitude AP's process to "discover" the Summit WM-Series Switch, the Summit WM-Series Switch Software system relies on a DHCP server that supports Option 78 and 79 for Service Location Protocol (SLP). The combination of Dynamic Host Configuration Protocol (DHCP), Option 78 and 79, and SLP provide a technique that defines the Summit WM-Series Switch as the only element on the network that the Altitude AP can communicate with.

Option 78 is a list of IP addresses of Directory Agents, used by Service Agents and Users Agents.

For the purposes of the Summit WM-Series Switch Software system, Option 78 should be set to the IP address of the Summit WM-Series Switch management port. The Summit WM-Series Switch will run the SLP daemon and act as a directory service.

NOTE

One of the ethernet ports on the Summit WM-Series Switch should be set to allow management traffic so that SLP messages can arrive on that port.

Option 79 is an identifier that refers to a set of services called a "scope". If a User Agent has been assigned to a scope, it can only see the services in that scope. This will limit the IP addresses of Directory Agents available to the User Agent.

Here's how Summit WM-Series Switch Software uses these SLP options:

1. The Summit WM-Series Switch Manager or the Altitude AP Manager use the Service Agent:
   - to look up the location of the Directory Agent using Option 78 and 79 in the DHCP server
   - to register with the Directory Agent
2. The Altitude AP User Agent looks up the location of the Directory Agent using Option 78 and 79 in the DHCP server.
3. The Altitude AP User Agent contacts the Directory Agent for services of the types "extreme".
4. The Altitude AP attempts to connect with the Summit WM-Series Switch or Altitude AP Manager.

Now the use of SLP is completed and the Altitude AP and Summit WM-Series Switch will now communicate using a UDP-based tunneling protocol.

Service Location Protocol (SLP) (RFC2608)

Service Location Protocol (RFC2608) is a method of organizing and locating the resources (such as printers, disk drives, databases, e-mail directories, and schedulers) in a network. Using SLP, networking applications can discover the existence, location and configuration of networked devices.

In larger installations, services will register their services with one or more Directory Agents, and clients will contact the Directory Agent to fulfill requests for Service Location information.

Service Location Protocol consists of three cooperating services:

- User Agent (UA): A process working on the user's behalf to acquire service attributes and configuration. The User Agent retrieves service information from the Service Agents or Directory Agents.
- Service Agent (SA): A process working on the behalf of one or more services to advertise service attributes and configuration.
- Directory Agent (DA): A process which collects information from Service Agents to provide a single repository of service information in order to centralize it for efficient access by User Agents. There can only be one DA present per given host.

When a service starts on the network, its Service Agent will query the DHCP server for Option 78 and 79 and will register itself appropriately.

DHCP Options for Service Location Protocol (RFC2610)

The Dynamic Host Configuration Protocol (RFC2131) provides a framework for passing configuration information to hosts on a TCP/IP network.

Entities using the Service Location Protocol, Version 2 (RFC2608) and Service Location Protocol, Version 1 (RFC2165) need to obtain the address of Directory Agents in order to transact messages. The SLP Directory Agent option described below (Option 78) is used to configure User Agents and Service Agents with the location of Directory Agents in the network.

The SLP Scope Option (Option 79) provides an assignment of scope for configuration of SLP User and Service Agents. This option takes precedence over both default and static scope configuration of SLP agents. A scope is a set of services, typically making up a logical administrative group.

SLP Directory Agent Option (Option 78)

The SLP Directory Agent Option 78 specifies a list of IP addresses for SLP Directory Agents. Directory Agents should be listed in order of preference.

The Length value must include one for the 'Mandatory' byte and include four for each Directory Agent address which follows. The address of the Directory Agent is given in network byte order. The 'Mandatory' byte in the Directory Agent option may be set to either 0 or 1. If it is set to 1, the SLP User Agent or Service Agent so configured must not employ either active or passive multicast discovery of Directory Agents.

The Directory Agents listed in Option 78 must be configured with the a non-empty subset of the scope list that the Agent receiving the Directory Agent Option 78 is configured with.

SLP Service Scope Option (Option 79)

Services are grouped together using 'scopes'. These are strings that identify a set of services that form an administrative grouping. Service Agents (SAs) and Directory Agents (DAs) are always assigned a scope string.

A User Agent (UA) is normally assigned a scope string (in which case the User Agent will only be able to discover that particular grouping of services). This allows a network administrator to provision services to users. The use of scopes also allows the administrator to scale SLP deployments to larger networks.

The Scope-List String is a comma-delimited list of the scopes that a SLP Agent is configured to use. The Length value must include one for the 'Mandatory' byte.

The 'Mandatory' byte determines whether SLP Agents override their static configuration for scopes with the <Scope List> string provided by the option. This allows DHCP administrators to implement a policy of assigning a set of scopes to Agents for service provision. If the Mandatory byte is 0, static configuration takes precedence over the DHCP provided scope list. If the Mandatory byte is 1, the <Scope List> provided in this option must be used by the SLP Agent.

The Scope List String usage is defined in the SLPv2 specification (RFC2608).

D Reference lists of standards

RFC list

Listed below are the Internet Engineering Task Force (IETF) Request for Comments (RFCs) standards supported by Summit WM-Series Switch Software.

The Request for Comments, a series of notes about the Internet, submitted to the Internet Engineering Task Force (IETF) and designated by an RFC number, that may evolve into an Internet standard. The RFCs are catalogued and maintained on the IETF RFC website: www.ietf.org/rfc.html.

Table 8: List of RFCs

RFC Number	Title
RFC 791	IPv4
RFC 1812	Minimum Router Requirements
RFC 793	Transport Control Protocol (TCP)
RFC 768	User Datagram Protocol (UDP)
RFC 792	Internet Control Message Protocol (ICMP)
RFC 826	Address Resolution Protocol (ARP)
RFC 2865	Remote Access Dial In User Service (RADIUS)
RFC 2866	RADIUS Accounting
RFC 2165, 2608	Service Location Protocol (SLP)
RFC 2131	Dynamic Host Configuration Protocol (DHCP)
RFC 2328	Open Shortest Path First (OSPF v2)
RFC 1587	OSPF Not So Stubby Area (NSSA) Option
RFC1350:	The TFTP Protocol (Revision 2)
RFC 2716	EAP-TLS
RFC 1155	Structure and identification of management information for TCP/IP-based internets.
RFC 1157	Simple Network Management Protocol (SNMP).
RFC 1212	Concise MIB definitions.
RFC 1213	Management Information Base for Network Management of TCP/IP-based internets MIB-II.
RFC 1215	Convention for defining traps for use with the SNMP.
RFC 1901	Introduction to Community-based SNMPv2 (SNMPv2c).
RFC 2011	SNMPv2 Management Information Base for the Internet Protocol using SMIv2.
RFC 2012	SNMPv2 Management Information Base for the Transmission Control Protocol using SMIv2.
RFC 2013	SNMPv2 Management Information Base for the User Datagram Protocol using SMIv2.
RFC 2578	Structure of Management Information Version 2 (SMIv2).
RFC 2579	Textual Conventions for SMIv2. 2580 Conformance Statements for SMIv2.
RFC 2863	The Interfaces Group MIB.

Table 8: List of RFCs (Continued)

RFC Number	Title
RFC 3416	Version 2 of the Protocol Operations for the Simple Network Management Protocol (SNMP)
RFC 3417	Transport Mappings for the Simple Network Management Protocol (SNMP).
RFC 3418	Management Information Base (MIB) for the Simple Network Management Protocol (SNMP).
RFC 959	File Transfer Protocol. (FTP)
RFC 2660	The Secure HyperText Transfer Protocol (HTTPS)
RFC 2030	Simple Network Time Protocol v4
RFC 1191	Path MTU Discovery
Internet Draft	Secure Shell v2 (SSHv2)
Internet Draft	EAP-TTLS
Internet Draft	EAP-PEAP
Internet Draft	CAPWAP Tunneling Protocol (CTP)

802.11 standards list

Also supported are the following 802.11 standards:

Table 9: List of 802.11 standards supported

Standard	Name	
802.11	Wireless LAN MAC and PHY Specifications	
802.11a	Wireless LAN	High Speed Physical Layer in 5 GHz band
802.11b	Wireless LAN	High Speed Physical Layer in 2.4 GHz band
802.11d	802.11 Extensions to Operate in Additional Regulatory Domains	
802.11g	Wireless LAN	Further High Data Rate Extensions in 2.4 GHz band
802.11h	Spectrum managed 802.11a (in 5 GHz band in Europe)	
802.11i	WLAN security and provide better network access control	
802.1x	Port based network access control	
802.11e	MAC Enhancements for Quality of Service (future)	
802.1aa	802.1x maintenance	
802.3af	DTE Power via MDI (Power over Ethernet)	
802.3	CSMA/CD (Ethernet)	
802.3i	10Base-T	
802.3u	100Base-T	
802.3x	Full Duplex	

Table 9: List of 802.11 standards supported (Continued)

Standard	Name	
802.3z	1000Base-X (Gigabit Ethernet)	
802.1d	MAC bridges	
802.11	MIB management information base for 802.11	

E Support for Altitude AP

Altitude AP diagnostics by Telnet

WARNING!

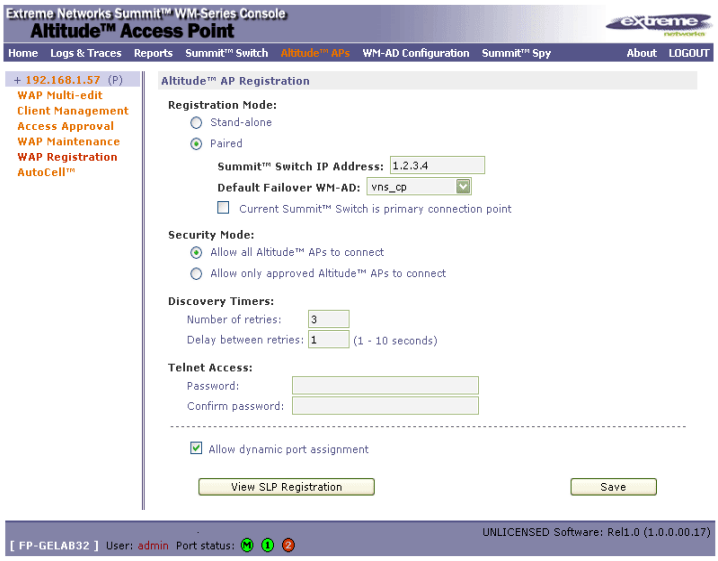
For security reasons, Telnet is disabled by default. Only enable it in order to perform a diagnostic session. When finished, disable Telnet again.

As a support tool to perform diagnostic debugging of the Altitude AP, the capability to access the Altitude AP by Telnet has been provided.

Normally Telnet is disabled and should be disabled again after diagnostics. This process should only be used by support services.

The process to enable Telnet access has two steps.

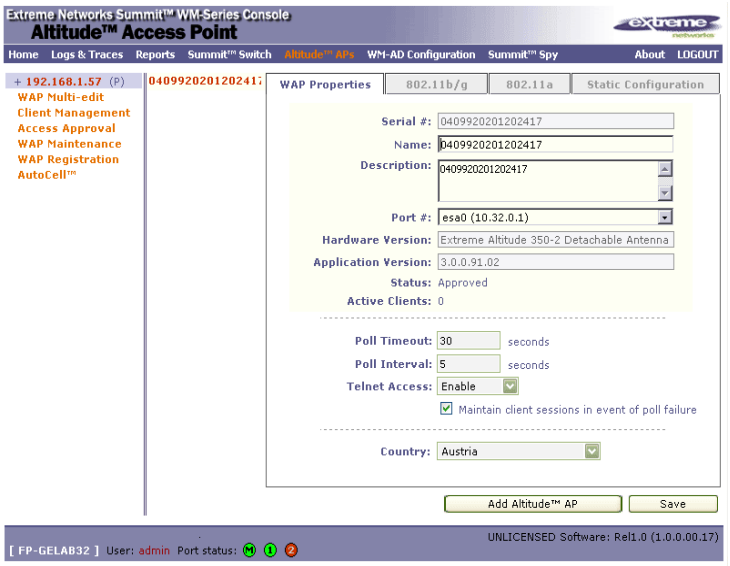
Use the *AP Registration* screen to set up password configuration for Telnet on the Altitude AP:



1 In the **Telnet Access** Password entry field, key in the password for a Telnet session. To confirm the password, key it in again.

2 To send the password information to all registered Altitude APs, click on the **Save** button.

Use the *AP Properties* screen, to enable Telnet on a selected Altitude AP.



1 Highlight the selected Altitude AP in the left-hand list.

2 In the **Telnet Access** field, select “Enable” from the drop-down list.

3 Click on the **Save** button.

You can now begin a Telnet session on this Altitude AP.

When the diagnostics are finished, disable Telnet access as follows:

1 In the **Telnet Access** field, select “Disable” from the drop-down list.

2 Click on the **Save** button.

F RADIUS Attributes

Remote Authentication Dial-In User Service (RADIUS) is an industry standard for providing identification, authentication, authorization, and accounting services for distributed dial-up/remote access networking.

RADIUS Vendor-Specific Attributes (VSAs)

RADIUS Vendor-Specific Attributes (VSAs) are RADIUS Authentication and Accounting attributes defined by vendors to customize information exchanges between clients and servers. This allows unique behaviors to be implemented in client applications without requiring custom server development. VSA support is included directly in dictionary files distributed with RADIUS server product (for example, with Funk Steel Belted RADIUS), or can be configured manually on most server products.

The following defines the Extreme Networks VSAs currently implemented in the Summit WM-Series Switch Software solution, defined using the Extreme Networks Organizationally Unique Identifier (OUI):

ID	Attribute Name	Type	Messages	Description
1	Extreme Network-URL-Redirection	string	Returned from RADIUS server	A URL that can be returned to redirect a session to a specific Web page.
2	Extreme Networks-AP-Name	string	Sent to RADIUS server	The name of the AP the client is associating to. It can be used to assign policy based on AP name or location.
3	Extreme Networks-AP-Serial	string	Sent to RADIUS server	The AP serial number. It can be used instead of (or in addition to) the AP name.
4	Extreme Networks-VNS-Name	string	Sent to RADIUS server	The name of the Virtual Network the client has been assigned to. It is used in assigning policy and billing options, based on service selection.
5	Extreme Networks-SSID	string	Sent to RADIUS server	The name of the SSID the client is associating to. It is used in assigning policy and billing options, based on service selection.
6	Extreme Networks-BSS-MAC	string	Sent to RADIUS server	The name of the BSS-ID the client is associating to. It is used in assigning policy and billing options, based on service selection and location.

RADIUS Accounting

Account-Start Packet

The following table lists the information elements (including VSAs) supported in a RADIUS Start message, issued by Summit WM-Series Switch Software, with RADIUS Accounting enabled:

Attribute	NO.	RAD. Data Type	Name
Acct-Session-Id	44	string	mu_session_id
User-Name	1	string	mu_user_id
Filter-Id	11	string	Filter-Id (Accept-response)
Acct-Interim-Interval	85	integer	(Accept-response/GUI input)
Session-Timeout	27	integer	(Accept-response/GUI input)
Class	25	octets	(Accept-response)
Login-LAT-Group	36	octets	(Accept-response)
Acct-Status-Type	40	integer	Start
Acct-Authentic	45	integer	Radius/Local/Remote
Framed-IP-Address	8	ipaddr	Mu_ip_address
Connect-Info	77	string	802.11 a[b][g]
NAS-port-type	61	integer	18/19
Called-Station-ID	30	string	BP MAC
Calling-Station-ID	31	string	mu_mac_address
Acct-Delay-Time	41	integer	
BP-Serial	VSA	string	Extreme Networks-AP-Serial
BP-Name	VSA	string	Extreme Networks-AP-Name
VNS-Name	VSA	string	Extreme Networks-VNS-Name
SSID	VSA	string	Extreme Networks-SSID

Account-Stop/Interim Packet

The following table lists the information elements (including VSAs) supported in a RADIUS Stop or Interim messages, issued by Summit WM-Series Switch Software, with RADIUS Accounting enabled:

Attribute	NO.	RAD. Data Type	Name
Acct-Session-Id	44	string	mu_session_id
User-Name	1	string	mu_user_id
Filter-Id	11	string	Filter-Id (Accept-response)
Acct-Interim-Interval	85	integer	(Accept-response/GUI input)
Session-Timeout	27	integer	(Accept-response/GUI input)
Class	25	octets	(Accept-response)
Login-LAT-Group	36	octets	(Accept-response)
Acct-Status-Type	40	integer	Stop/Interim-Update
Acct-Authentic	45	integer	Radius/Local/Remote
Framed-IP-Address	8	ipaddr	Mu_ip_address
Connect-Info	77	string	802.11 a[b][g]
NAS-port-type	61	integer	18/19
Called-Station-ID	30	string	BP MAC
Calling-Station-ID	31	string	mu_mac_address
Acct-Delay-Time	41	integer	
Acct-Session-Time	46	integer	
Acct-Input-Packets	47	integer	
Acct-Output-Packets	49	integer	
Acct-Input-Octets	42	integer	
Acct-Output-Octets	43	integer	
Acct-Input-Gigawords	52	integer	
Acct-Output-Gigawords	53	integer	
Acct-Terminate-Cause	49	integer	
BP-Serial	VSA	string	Extreme Networks-AP-Serial
BP-Name	VSA	string	Extreme Networks-AP-Name
VNS-Name	VSA	string	Extreme Networks-VNS-Name
SSID	VSA	string	Extreme Networks-SSID

Termination Codes

The RADIUS client (SWM or AP) terminates the wireless device user's session when one of the following events occur:

- user request
- idle timeout
- session timeout
- administrator reset

When a user session is terminated, the RADIUS client sends a RADIUS accounting stop request that will include one of the following termination codes:

Radius Value	Radius Definition	XP Value	XP/SMT Definition	XP Name
1	User Request	9	RF notification that MU has disconnected from RU. This would be the case if there is a Logoff button for Captive Portal. Normally this would not apply to 802.1x connections.	MU_DEREG_REASON_USER_REQUEST
4	Idle Timeout	1	User has been disconnected due to idle timeout and inactivity	MU_DEREG_REASON_IDLE_TIMEOUT
5	Session Timeout	7	Disconnection as a result of the maximum session length value returned by the RADIUS server upon successful authentication.	MU_DEREG_REASON_LIFETIME_TIMEOUT
6	Admin Reset	2	Explicit request by Management infrastructure (GUI user) to disconnect MU	MU_DEREG_REASON_RF_DICONNECT
		3		MU_DEREG_REASON_ADMIN_REQ
		8		MU_DEREG_REASON_TUNNEL_DISCONNECT
11	NAS Reboot		BM graceful shutdown	N/A
17	User Error		Unknown reason	N/A

G Logs and Events

Overview

The Summit WM-Series Switch is designed to behave like an appliance. It is either in an operational state, or it has failed due to a hardware problem or low level packet processing issue. In general, the system will self recover by rebooting if the system fault is recoverable.

There are two main monitoring processes in the system:

- a hardware watchdog
- a software watchdog

The software watchdog restarts stalled or failed processes, while the hardware watchdog causes system reboot should the software watchdog fail. The result of this approach is that little intervention is required once the system is properly configured and operational.

Critical

The following subsections contain tables describing all Critical log messages. The sections are listed alphabetically by Component Name.

ACCESSPOINT

ACCESSPOINT	
Severity	Critical
Log Message	AccessPoint software upgrade failed. Cannot find out flash free space.
Description	AccessPoint software upgrade failed.
Action	Make sure to have the proper Access Point software file on AC for downloading .

ACCESSPOINT	
Severity	Critical
Log Message	AccessPoint software upgrade failed. Not enough flash space for backup file.
Description	AccessPoint software upgrade failed.
Action	Make sure to have the proper Access Point software file on AC for downloading .

ACCESSPOINT	
Severity	Critical
Log Message	AccessPoint software upgrade failed. Cannot open application backup file.
Description	AccessPoint software upgrade failed.
Action	Make sure to have the proper Access Point software file on AC for downloading .

ACCESSPOINT	
Severity	Critical
Log Message	AccessPoint software upgrade failed. Writing backup file failed
Description	AccessPoint software upgrade failed.
Action	Make sure to have the proper Access Point software file on AC for downloading .

ACCESSPOINT	
Severity	Critical
Log Message	AccessPoint software upgrade failed. File small or ELF header corrupted.
Description	AccessPoint software upgrade failed.
Action	Make sure to have the proper Access Point software file on AC for downloading .

ACCESSPOINT	
Severity	Critical
Log Message	AccessPoint software upgrade failed. File wrong size.
Description	AccessPoint software upgrade failed.
Action	Make sure to have the proper Access Point software file on AC for downloading .

ACCESSPOINT	
Severity	Critical
Log Message	AccessPoint configuration failed. Wassp config rcv: cannot decode tlv packet.
Description	AccessPoint configuration failed
Action	Check software and configuration compatibility. Check the connection to AP.

ACCESSPOINT	
Severity	Critical
Log Message	AccessPoint configuration failed. Wassp config rcv: config missing from tlv packet.
Description	AccessPoint configuration failed
Action	Check software and configuration compatibility. Check the connection to AP.

ACCESSPOINT	
Severity	Critical
Log Message	AccessPoint configuration failed. Wassp config rcv: cannot send config to SNMP Agent.
Description	AccessPoint configuration failed
Action	Check software and configuration compatibility. Check the connection to AP.

ACCESSPOINT	
Severity	Critical
Log Message	AccessPoint configuration failed. Wassp config rcv: cannot get response from SNMP Agent.
Description	AccessPoint configuration failed
Action	Check software and configuration compatibility. Check the connection to AP.

ACCESSPOINT	
Severity	Critical
Log Message	AccessPoint configuration failed. Wassp config rcv: received error in Response from SNMP Agent.
Description	AccessPoint configuration failed
Action	Check software and configuration compatibility. Check the connection to AP.

ACCESSPOINT	
Severity	Critical
Log Message	AccessPoint Rebooting. Radio Interference detected in channel 2.
Description	AccessPoint Rebooting.
Action	AP detected a problem and rebooted automatically. Check the log message detail. No action is normally needed.

ACCESSPOINT	
Severity	Critical
Log Message	AccessPoint Rebooting. Radar interference is detected.
Description	AccessPoint Rebooting.
Action	AP detected a problem and rebooted automatically. Check the log message detail. No action is normally needed.

ACCESSPOINT	
Severity	Critical
Log Message	AccessPoint Rebooting. Radar detected.
Description	AccessPoint Rebooting.
Action	AP detected a problem and rebooted automatically. Check the log message detail. No action is normally needed.

ACCESSPOINT	
Severity	Critical
Log Message	AccessPoint Rebooting. AP-AC poll timeout.
Description	AccessPoint Rebooting.
Action	AP detected a problem and rebooted automatically. Check the log message detail. No action is normally needed.

ACCESSPOINT	
Severity	Critical
Log Message	AccessPoint Rebooting. ChipReset: Error resetting WLAN HW.
Description	AccessPoint Rebooting.
Action	AP detected a problem and rebooted automatically. Check the log message detail. No action is normally needed.

ACCESSPOINT	
Severity	Critical
Log Message	AccessPoint Rebooting. Error resetting WLAN HW during mode change.
Description	AccessPoint Rebooting.
Action	AP detected a problem and rebooted automatically. Check the log message detail. No action is normally needed.

ACCESSPOINT	
Severity	Critical
Log Message	AccessPoint Rebooting. AP Discovery timeout AFTER 5 MINUTES.
Description	AccessPoint Rebooting.
Action	AP detected a problem and rebooted automatically. Check the log message detail. No action is normally needed.

ACCESSPOINT	
Severity	Critical
Log Message	AccessPoint Rebooting. AP Unable to allocate memory.
Description	AccessPoint Rebooting.
Action	AP detected a problem and rebooted automatically. Check the log message detail. No action is normally needed.

ACCESSPOINT	
Severity	Critical
Log Message	AccessPoint Running Backup image File size is 1500222.
Description	AccessPoint Running Backup image.
Action	AP could not run the latest installed software and is running the backup software instead. Upgrade AP with the proper latest software.

CDR_COLLECTOR

CDR_COLLECTOR	
Severity	Critical
Log Message	CDR Manager failed to open accounting file for writing. The CDR Manager will halt.
Description	The accounting record file could not be opened; as accounting records cannot be written, the service halted.
Action	Indicates that the accounting record partition is corrupted. Contact service as the controller may require servicing.

CDR_COLLECTOR	
Severity	Critical
Log Message	Memory allocation failure - unable to generate accounting record. CDR Manager will halt.
Description	Indicates that the system memory has been corrupted.
Action	In normal operating circumstances, the entire system behaves erratically, if functioning at all. Contact service as the system may need to be replaced.

CDR_COLLECTOR	
Severity	Critical
Log Message	File storage limit has been reached for the accounting files. The oldest file(s) will be deleted to free up room for the new accounting files.
Description	Indicates that the system memory has been corrupted.
Action	In normal operating circumstances, the entire system behaves erratically, if functioning at all. Contact service as the system may need to be replaced.

CDR_COLLECTOR	
Severity	Critical
Log Message	File storage limit has been reached for the accounting files. The oldest file(s) will be deleted to free up room for the new accounting files.
Description	Indicates that a large number of accounting records have been stored within the 7 day turn-over period. This notification indicates that to keep processing, records will be deleted.
Action	Copy off the relevant data records to ensure that accounting information is not lost.

CONFIG_MANAGER

CONFIG_MANAGER	
Severity	Critical
Log Message	Config Manager has suffered a critical error and will halt.
Description	Indicates a memory allocation failure.
Action	In normal operating circumstances, the entire system behaves erratically, if functioning at all. Contact service as the system may need to be replaced.

CONFIG_MANAGER	
Severity	Critical
Log Message	Access point controlled software upgrade has failed. This normally occurs if a corrupt image file was selected as the upgrade image. Please select another image for the upgrade: %s
Description	AP upgrade has failed due to a bad software image.
Action	The selected upgrade image has a problem. Select a known good image and apply it to the access points for upgrade. Normally, this error results from the original image having been obtained via FTP without the "bin" directive.

CONFIG_MANAGER	
Severity	Critical
Log Message	Access point automatic software upgrade/downgrade has failed. This normally occurs if a corrupt image file was selected as the default image. Please select another default image. This alarm will repeat as long as the system is in automatic mode: %s
Description	Automatic AP upgrade request has failed due to a bad software image.
Action	The selected upgrade image has a problem. Select a known good image and apply it to the access points for upgrade. Normally, this error results from the original image having been obtained via FTP without the "bin" directive.

EVENT_SERVER

EVENT_SERVER	
Severity	Critical
Log Message	Cannot access logging file. Unable to save any system log messages.
Description	Unable to open log files for message storage.
Action	Indicates a low level file system problem, or the file permissions may have been altered. Check the file permissions first. If they appear to be correct, the file system may be corrupted. Log messages should still be forwarded to syslog and SNMP if services are enabled.

EVENT_SERVER	
Severity	Critical
Log Message	Critical internal error - log file protection flags have been corrupted. Event server will halt.
Description	File system has encountered a problem and the log file cannot be opened for writing.
Action	Indicates that the logging partition is corrupted. Contact service as the controller may require servicing.

EVENT_SERVER	
Severity	Critical
Log Message	Internal system interrupt handlers failed to initialize. Event server will halt.
Description	Internal service failure.
Action	In normal operating circumstances, the entire system behaves erratically, if functioning at all. Contact service s the system may require servicing.

EVENT_SERVER	
Severity	Critical
Log Message	Unable to initialize internal program thread. Event server will halt.
Description	Internal service failure
Action	In normal operating circumstances, the entire system behaves erratically, if functioning at all. Contact service as the system may need to be replaced.

EVENT_SERVER	
Severity	Critical
Log Message	Memory allocation failure. Unable to log last event.
Description	Indicates a memory allocation failure.
Action	In normal operating circumstances, the entire system behaves erratically, if functioning at all. Contact service as the system may need to be replaced.

EVENT_SERVER	
Severity	Critical
Log Message	Socket call failed. Will not be able to communicate with specific component. Error no: %d.
Description	Inter-component communication failure.
Action	Indicates that a service the event server depends on has failed. There may be another event from the Start-up Manager indicating that a service has been restarted.

EVENT_SERVER	
Severity	Critical
Log Message	Socket select error - 100% CPU utilization can occur and overall system performance will be impaired.
Description	Internal communication error.
Action	Shell into the O/S and kill the process. Report event to service.

EVENT_SERVER	
Severity	Critical
Log Message	The evaluation license for the controller has expired. Please contact your customer representative and purchase licenses to continue using the controller. If you do not purchase a license, the legal requirement is to put the system out of service.
Description	Licensing infrastructure.
Action	Acquire a valid license for the system to ensure legal operation of the equipment.

LANGLEY

LANGLEY	
Severity	Critical
Log Message	Langley has suffered a critical error, and has halted. Error Details: %s
Description	Messaging infrastructure alarm.
Action	If this error appears, the system is completely non-functional. The hardware watchdog timer will kick in and the system will reboot. If the error persists, contact service as the system may need to be replaced.

RADIUS_ACCOUNTING

RADIUS_ACCOUNTING	
Severity	Critical
Log Message	No Response from all RADIUS accounting server(s): %s.
Description	External RADIUS Accounting server access has been interrupted.
Action	Indicates that network connectivity needs to be checked. The system is operating correctly, but the external connections have been lost. Therefore, no RADIUS accounting records can be saved for the client sessions.

RADIUS_CLIENT

RADIUS_CLIENT	
Severity	Critical
Log Message	A file system error occurred. Unable to open RADIUS dictionary file. RADIUS client exiting.
Description	The file system has encountered a problem and the RADIUS dictionary file cannot be opened for reading.
Action	Indicates that the main service partition is corrupted, or there has been a low level file error. Alternatively, the file permissions may have been altered. First check the file permissions; if they appear correct, contact service as the controller may need servicing.

RADIUS_CLIENT	
Severity	Critical
Log Message	Cannot allocate memory for either Captive Portal and/or EAP modules. RADIUS client exiting.
Description	Indicates a memory allocation failure.
Action	In normal operating circumstances, the entire system will most likely behave erratically if it functions at all. Contact service as the system may need to be replaced.

RADIUS_CLIENT	
Severity	Critical
Log Message	Failed to send process status success to Startup Manager. Start-up Manager will reboot the RADIUS client.
Description	Interprocess communication failure.
Action	No action required.

RADIUS_CLIENT	
Severity	Critical
Log Message	No radius server available for VNS: %s.
Description	None of the RADIUS servers configured for a VNS are reachable by the RADIUS client.
Action	Indicates that network connectivity needs to be checked. The system is operating correctly, but the external connections have been lost. No RADIUS servers can be contacted for client authentication.

RF_DATA_COLLECTOR

RF_DATA_COLLECTOR	
Severity	Critical
Log Message	An error has occurred in the RF Data Collector which will cause this component to shutdown (and be restarted by the system). Details:%s.
Description	Indicates an internal service failure.
Action	Monitor the system for re-occurrences. If it appears under similar operating circumstances, there may be data corruption in the network. If other parts of the controller begin to behave erratically, this may indicate a hardware failure. Contact service as the controller may need servicing.

RU_MANAGER

RU_MANAGER	
Severity	Critical
Log Message	RU Manager has suffered a critical internal error and will halt (unable to start process thread).
Description	Indicates an internal service failure.
Action	In normal operating circumstances, the entire system behaves erratically, if functioning at all. Contact service as the system may need to be replaced.

RU_MANAGER	
Severity	Critical
Log Message	RU Manager has suffered a critical internal error and will halt (unable to open data dictionary).
Description	The file system has encountered a problem, and the messaging data dictionary file cannot be opened for reading.
Action	Indicates that the main service partition is corrupted, or there has been a low level file error. Alternatively, the file permissions may have been altered. First check the file permissions; if they appear correct, contact service as the controller may need servicing.

RU_MANAGER	
Severity	Critical
Log Message	AC Manager: Moving into failover mode
Description	The controller is in availability mode, and the paired controller has failed. The system is moving into fail-over mode.
Action	Investigate failure of other controller to return environment to normal operation.

SECURITY_MANAGER

SECURITY_MANAGER	
Severity	Critical
Log Message	Cannot allocate memory. Will not be able to process Captive portal authentication request.
Description	Indicates a memory allocation failure.
Action	In normal operating circumstances, the entire system behaves erratically, if functioning at all. Contact service as the system may need to be replaced.

SECURITY_MANAGER	
Severity	Critical
Log Message	Failed to initialize list of session tracking tags (token). Will not be able to process Captive portal authentication requests.
Description	Indicates a memory allocation failure for a specific program function.
Action	In normal operating circumstances, the entire system behaves erratically, if functioning at all. Contact service as the system may need to be replaced.

SECURITY_MANAGER	
Severity	Critical
Log Message	Unable to open listening socket. Will not be able to communicate with Apache server.
Description	Inter-component communication failure.
Action	Verify that the web server is still running. If it is, re-start the security manager process to clear the problem.

SECURITY_MANAGER	
Severity	Critical
Log Message	Error binding to listener socket. Will not be able to communicate with Apache server.
Description	Inter-component communication failure.
Action	Verify that the web server is still running. If it is, re-start the security manager process to clear the problem.

SECURITY_MANAGER	
Severity	Critical
Log Message	Listen call failed. Will not be able to communicate with Apache Server.
Description	Inter-component communication failure.
Action	Verify that the web server is still running. If it is, re-start the security manager process to clear the problem.

SECURITY_MANAGER	
Severity	Critical
Log Message	Socket call failed. Will not be able to communicate with specific component.
Description	Inter-component communication failure.
Action	Indicates that a service the Security Manager depends on has failed. There may be another event from the Start-up Manager indicating that a service has been restarted.

STARTUP_MANAGER

STARTUP_MANAGER	
Severity	Critical
Log Message	Failed attempting to start router ports. System reboot initiated.
Description	Hardware initialization error.
Action	The router ports could not be initialized. The system reboots to attempt recovery. If the problem does not clear, Contact service as the system may need to be replaced.

STARTUP_MANAGER	
Severity	Critical
Log Message	Internal connection to router ports lost. Restart initiated.
Description	Hardware failure.
Action	Communication path to the router ports is lost. Reboot the system to attempt recovery.

STARTUP_MANAGER	
Severity	Critical
Log Message	HSM failed to start. System reboot initiated.
Description	Major system process start failure
Action	The process responsible for starting the interface IP stack failed to start. The system is rebooted automatically to attempt to clear the problem. If failure persists, try installing a previous version of the system software. If this fails to clear the problem, contact service as the operating system has failed or the base line configuration files have been corrupted.

STARTUP_MANAGER	
Severity	Critical
Log Message	HSM is down. System reboot initiated
Description	Major system process failure
Action	The process responsible for managing the interface IP stack failed. The system is rebooted automatically to attempt to clear the problem. If failure persists, try installing a previous version of the system software. If this fails to clear the problem, contact service as the operating system has failed or the base line configuration files have been corrupted.

STARTUP_MANAGER	
Severity	Critical
Log Message	HSM failed to reply to status notification. System reboot initiated.
Description	Major system process failure
Action	The process responsible for managing the interface IP stack failed. The system is rebooted automatically to attempt to clear the problem. If failure persists, try installing a previous version of the system software. If this fails to clear the problem, contact service as the operating system has failed or the base line configuration files have been corrupted.

STARTUP_MANAGER	
Severity	Critical
Log Message	Failed to connect to Langley. System reboot initiated.
Description	Messaging infrastructure could not start.
Action	The messaging system has failed. The system is rebooted automatically to attempt to clear the problem. If failure persists, try installing a previous version of the system software. If this fails to clear the problem, contact service as the box may need to be replaced.

STATS_SERVER

STATS_SERVER	
Severity	Critical
Log Message	Statistics Server suffered an internal connection failure. Retrying connection in 5 seconds.
Description	Process could not connect to internal messaging infrastructure.
Action	Indicates that the process cannot connect to the message bus. The system may behave erratically at this point. Shell into the O/S and kill the process to see if that clears the problem. If the problem does not clear, try downgrading to a previous software release.

VNMGR

VNMGR	
Severity	Critical
Log Message	Critical internal error - memory protection flags have been corrupted. VN Manager will halt.
Description	Indicates that internal memory protection flags have been corrupted.
Action	If the process did not restart after emitting this error, or if client association, MAC-based authentication, or mobility problems continue to exist, shell into the O/S and kill the process to see if that clears the problem. If the problem does not clear, try downgrading to a previous software release

VNMGR	
Severity	Critical
Log Message	Internal system interrupt handlers failed to initialize. VN Manager will halt.
Description	Indicates that internal system interrupt handlers have failed to initialize.
Action	If the process did not restart after emitting this error, or if client association, MAC-based authentication, or mobility problems continue to exist, shell into the O/S and kill the process to see if that clears the problem. If the problem does not clear, try downgrading to a previous software release

VNMGR	
Severity	Critical
Log Message	Unable to initialize internal program thread. VN Manager will halt.
Description	Indicates that the process cannot allocate or update process threads.
Action	If the process did not restart after emitting this error, or if client association, MAC-based authentication, or mobility problems continue to exist, shell into the O/S and kill the process to see if that clears the problem. If the problem does not clear, try downgrading to a previous software release

VNMGR	
Severity	Critical
Log Message	Critical internal error - unable to allocate memory for VN Manager. VN Manager will halt.
Description	Indicates a memory allocation failure.
Action	If the process did not restart after emitting this error or if client association, MAC-based authentication, or mobility problems continue to exist, shell into the O/S and kill the process to see if that clears the problem. If the problem does not clear, try downgrading to a previous software release, where the memory leak may not exist.

VNMGR	
Severity	Critical
Log Message	Socket call failed. Will not be able to communicate with specific component.
Description	A socket call has failed, which may make the process unable to communicate with another process.
Action	This log may be generated after a normal restart of the process, a normal restart of the controller, or a change in the role for mobility, and in these cases can be ignored. If the log is generated outside of these cases, the process cannot communicate with another process. Shell into the O/S and kill the process to see if that clears the problem. If the problem does not clear, try downgrading to a previous software.

Major

The following subsections contain tables describing all Major log messages. The sections are listed alphabetically by Component Name.

ACCESSPOINT

ACCESSPOINT	
Severity	Major
Log Message	Communication with Access Controller lost. AP - AC poll timeout.
Description	AccessPoint poll timed out.
Action	Check the IP connection between Access controller and Access Point. If the Heartbeat between AC and AP timed out, check the configuration of AP poll and timeout periods.

ACCESSPOINT	
Severity	Major
Log Message	AccessPoint Problem Report captured. Ap-report-5.txt (size 37222 bytes).
Description	AccessPoint Problem Report captured.
Action	AP detected a problem and captured relevant data to a file. Upload ap-report file to Access controller and send it to field support. The file will be analyzed by Extreme Networks to resolve and correct the problem.

ACCESSPOINT	
Severity	Major
Log Message	AccessPoint software upgrade done. File size is 1500222.
Description	AccessPoint software upgrade done.
Action	None. AP software upgrade has been successfully completed.

ACCESSPOINT	
Severity	Major
Log Message	Beacon Creation Problem. Cannot allocate beacon.
Description	Beacon Creation Problem.
Action	Upgrade AP with the proper latest software.

CDR_COLLECTOR

CDR_COLLECTOR	
Severity	Major
Log Message	Internal messaging error: %d. Accounting information for one client session will be incomplete.
Description	Accounting record is incomplete for a single client session.
Action	A single accounting record is incomplete. To accurately bill for usage, the client session needs to be audited against the RADIUS accounting server.

CDR_COLLECTOR	
Severity	Major
Log Message	Can not create new CDR record for session%d. Accounting record for one client session will be unavailable.
Description	Transient error condition while creating an accounting record.
Action	A single accounting record is incomplete. To accurately bill for usage, the client session needs to be audited against the RADIUS accounting server.

CDR_COLLECTOR	
Severity	Major
Log Message	Error will be ignored and message re-tried.
Description	Error sending message on the system messaging infrastructure.
Action	Recoverable messaging error; the process will recover. Monitor for future occurrences, and contact support if the problem persists.

CDR_COLLECTOR	
Severity	Major
Log Message	Internal messaging error:%d. Error will be ignored and message re-tried.
Description	Process could not connect to internal messaging infrastructure.
Action	Recoverable messaging error; the process will recover. Monitor for future occurrences, and contact support if the problem persists.

CDR_COLLECTOR	
Severity	Major
Log Message	CDR Manager failed when attempting to write client record to accounting file. Accounting record for this client session will be unavailable.
Description	File input error.
Action	A single accounting record was not written to the accounting log. To accurately bill for usage, the client session needs to be audited against the RADIUS accounting server. Monitor for future occurrences, and contact support if the problem persists as it points to a file system corruption or that the accounting partition has been corrupted.

CDR_COLLECTOR	
Severity	Major
Log Message	Internal messaging error - more accounting records were received than expected. Known sessions will be processed; unknown information will be dropped.
Description	Valid message with unknown client information received.
Action	Indicates that a valid accounting message was received for an unknown client. The information will be dropped. It is recommended that the RADIUS accounting server be audited to verify accounting data accuracy.

CLI

CLI	
Severity	Major
Log Message	Upgrade process failed - failure reason:%s.
Description	Software maintenance error.
Action	Indicates that the attempted upgrade failed. Verify that the image is valid. Try downloading the image before upgrading.

CLI	
Severity	Major
Log Message	System restore process failed - failure reason:%s.
Description	System maintenance error.
Action	Failed to restore system to previous save point. Try another system restore file, or verify that the current restore has not been corrupted prior to being uploaded to the controller.

CLI	
Severity	Major
Log Message	Patch installation failed - failure reason:%s.
Description	Software maintenance error.
Action	Try applying a different patch, or verify that the patch has not been corrupted prior to being uploaded to the controller.

CONFIG_MANAGER

CONFIG_MANAGER	
Severity	Major
Log Message	Config Manager has experienced an error which has prevented it from properly processing a request. CM will continue running, however this error may be an indicator of a larger system problem. Error Details
Description	CM messaging error.
Action	Monitor the system for re-occurrence. If problem re-occurs, other components may report additional problems. Try rebooting system to clear problem, and contact support if the problem persists.

CONFIG_MANAGER	
Severity	Major
Log Message	Access point %s has reported a radar interference violation on %s. The affected radio(s) have been placed in auto channel select mode, and will not respond to channel changes until 30min after the radar interference is last detected.
Description	AP behavior message.
Action	No action required. However, the AP will appear as though it is out of service. The message is provided as an informational response to client queries regarding service outage.

CPDP_AGENT_ID

CPDP_AGENT_ID	
Severity	Major
Log Message	Possible LAND DoS attack (%s).
Description	Denial of service attack warning.
Action	Investigate the source of attack, and block offending system from the network.

CPDP_AGENT_ID	
Severity	Major
Log Message	Possible PING-OF-DEATH DoS attack (%s).
Description	Denial of service attack warning.
Action	Investigate source of attack, and block offending system from the network.

EVENT_SERVER

EVENT_SERVER	
Severity	Major
Log Message	The controller evaluation license will expire in %s days. Please contact your customer representative and purchase licenses to continue using the controller.
Description	License expiration warning
Action	See log message for appropriate action.

EVENT_SERVER	
Severity	Major
Log Message	Audit message error. Unable to log audit message.
Description	Logging behavior.
Action	An event from the web pages could not be logged. If problem persists, check logs for other related error messages.

EVENT_SERVER	
Severity	Major
Log Message	Unknown internal program message received - type %d. Message will be ignored and processing continued.
Description	Internal communications.
Action	No action required.

EVENT_SERVER	
Severity	Major
Log Message	Unable to open audit file - Error no: %d. Message will be dropped.
Description	Audit file open error.
Action	Indicates that the logging partition may be full or corrupted. Contact service.

EVENT_SERVER	
Severity	Major
Log Message	Unable to determine audit file size - Error no: %d. Message will be dropped.
Description	Audit file write error.
Action	Indicates that the logging partition may be full or corrupted. Contact service.

EVENT_SERVER	
Severity	Major
Log Message	Cannot reset audit file pointer to beginning of the audit file - Error no: %d. The message and subsequent messages will be dropped.
Description	Audit file circular buffer problem.
Action	Indicates that the audit file may be corrupted, or the logging partition is full or corrupted. Try deleting the audit file and restarting the event server.

EVENT_SERVER	
Severity	Major
Log Message	Cannot set audit file pointer to specific position in the log - Error no: %d. The message and subsequent messages will be lost.
Description	Audit file circular buffer problem.
Action	Indicates that the audit file could be corrupted or that the logging partition is full or corrupted. Try deleting the audit file and restarting the event server.

LANGLEY

LANGLEY	
Severity	Major
Log Message	Langley has experienced an error which has prevented it from properly processing a request. Langley will continue running, however this error may be an indicator of a larger system problem. Error Details: %s
Description	Internal messaging problem.
Action	No action required. However, monitoring for re-occurrence is recommended. Other event logs may indicate that a component has failed and been re-started.

LANGLEY	
Severity	Major
Log Message	A connection request from '%s' failed to authenticate with the messaging server. This may indicate that somebody is port-scanning the access controller, or is attempting to gain backdoor access.
Description	Internal messaging security warning.
Action	Block network access to the process or user that is attempting to connect to the messaging bus. This is an attempt to compromise the internal operation of the system.

NSM_SERVER

NSM_SERVER	
Severity	Major
Log Message	NSM suffered an internal connection failure. Re-trying connection.
Description	Internal communications error.
Action	No action required. Process should recover. If failure continues, try restarting process.

NSM_SERVER	
Severity	Major
Log Message	NSM suffered an internal messaging failure. Re-trying connection.
Description	Internal communications error.
Action	No action required. Process should recover. If failure continues, try restarting process.

OSPF_SERVER

OSPF_SERVER	
Severity	Major
Log Message	OSPF server suffered an internal messaging failure. Re-trying connection.
Description	Internal communications error.
Action	No action required. Process should recover. If failure continues, try restarting process.

PORT_INFO_J_MANAGER

PORT_INFO_J_MANAGER	
Severity	Major
Log Message	Next hop device is unreachable (%s)
Description	Network Connectivity problem
Action	Investigate network equipment problem. While the next hop route is down, no client traffic from the affected VNSs is being forwarded. All clients will have effectively lost wired service.

RADIUS_ACCOUNTING

RADIUS_ACCOUNTING	
Severity	Major
Log Message	No Response from one RADIUS accounting server: %s.
Description	RADIUS accounting server interaction.
Action	May indicate that a RADIUS accounting server is down or that network connectivity has been lost. Investigate to see if the network is working correctly, or if the RADIUS accounting server has unexpectedly failed.

RADIUS_CLIENT

RADIUS_CLIENT	
Severity	Major
Log Message	Failed to retrieve configuration from the Config Manager. Will retry connection to Config Manager.
Description	RADIUS client service information.
Action	No action required. The config manager process has not responded. System should recover.

RADIUS_CLIENT	
Severity	Major
Log Message	Radius server changed: %s
Description	RADIUS client service information.
Action	No action required

RADIUS_CLIENT	
Severity	Major
Log Message	Failed to get radius profile for VNS: %s.
Description	RADIUS client service information.
Action	No action required. The config manager process has not responded. System should recover.

REDIR_ID

REDIR_ID	
Severity	Major
Log Message	Redirect packet is too big, packet will be dropped (%s)
Description	Data path behavior.
Action	If this message appears, a client session has attempted to connect to a site with a very large initial target URL. As the buffer size for the URL redirect process has been exceeded, the packet is dropped. The client will not be redirected to the captive portal authentication screen. For the client to be successfully authenticated, they need to connect to a different web site before they will be re-directed.

RF_DATA_COLLECTOR

RF_DATA_COLLECTOR	
Severity	Major
Log Message	An error has occurred in the RF Data Collector. This error will be ignored and the component will attempt to continue. Details: %s.
Description	RF_Data_collector service information.
Action	No action required; process should recover.

RU_MANAGER

RU_MANAGER	
Severity	Major
Log Message	An AP has attempted to connect that is unknown to the system. AP authentication failure. %s.
Description	Access point registration information.
Action	Indicates that someone may be attempting to set-up a rogue AP and/or spoof the registration/authentication process. It is recommended that the device be blocked from the network until the identity of the AP can be verified.

RU_MANAGER	
Severity	Major
Log Message	AP fails discovery. %s
Description	Access point registration information
Action	No action required; AP will come back through discovery. However, this message may also indicate that an unsupported AP version is attempting to connect to the system. If this is the case, an older version of the system software must be installed and the AP upgraded to a software version that can register with the current version.

SECURITY_MANAGER

SECURITY_MANAGER	
Severity	Major
Log Message	Status thread failed to start. It is unable to communicate with startup/shutdown Manager until status thread starts.
Description	Security Manager service information.
Action	No action required; process will recover or will be automatically restarted.

SECURITY_MANAGER	
Severity	Major
Log Message	Error occurred when sending response message to Apache server.
Description	Security Manager service information.
Action	If this occurs, a client session will fail captive portal authentication. The end user should try to authenticate again. Alternatively, try restarting the process to see if this clears the problem.

SECURITY_MANAGER	
Severity	Major
Log Message	Unable to create new session tracking tag (token mapping) based on MAC address. Will not be able to process Captive portal authentication request.
Description	Security Manager service information.
Action	If this occurs, a client session will fail captive portal authentication. The end user should try to authenticate again. Alternatively, try restarting to the process to see if this clears the problem.

SECURITY_MANAGER	
Severity	Major
Log Message	Get next available session tracking tag (token) returns zero. Will not be able to process Captive portal authentication request.
Description	Security Manager service information.
Action	If this occurs, a client session will fail captive portal authentication. The end user should try to authenticate again. Alternatively, try restarting to the process to see if this clears the problem.

SECURITY_MANAGER	
Severity	Major
Log Message	Error on deleting session tracking tag (token) %d. This will not impact success/failure of authentication request - it may create a memory leak if multiple tokens cannot be deleted.
Description	Security Manager service information.
Action	No action required. If the failure frequently re-occurs, it may be useful to restart the process to free lost memory.

SECURITY_MANAGER	
Severity	Major
Log Message	Unable to start component [%d]. Services provided by the component will be unavailable.
Description	System service status message.
Action	Try restarting the controller to see if that clears the problem. If rebooting does not clear the problem, contact support. Even though the process is down, it may not operationally effect the system. It may impair only parts of the system behavior.

SECURITY_MANAGER	
Severity	Major
Log Message	Component [%d] is down. Component will be restarted.
Description	System service status message.
Action	No action required.

SECURITY_MANAGER	
Severity	Major
Log Message	Component [%s] is down. Component will be restarted.
Description	System service status message.
Action	No action required.

VNMGR

VNMGR	
Severity	Major
Log Message	Configuration error - missing or bad parameters. VN Manager will retry configuration request. VN Manager will not start-up until configuration is successful.
Description	VN Manager status message.
Action	Verify that Config Manager is operational. Re-start if process has stopped. Problem should clear without intervention.

VNMGR	
Severity	Major
Log Message	Set Configuration data failed. The VNMgr may be restarted.
Description	VN Manager status message.
Action	No action required. Process should be restarted without intervention.

VNMGR	
Severity	Major
Log Message	Get Configuration data failed. The VNMgr may be restarted.
Description	VN Manager status message.
Action	No action required. Process should be restarted without intervention.

VNMGR	
Severity	Major
Log Message	VN Manager internal status changed. VN Manager will shutdown and be re-started by the Start-up Manager.
Description	VN Manager status message.
Action	VN Manager has been changed from Agent to Manager or vice-versa. No action required.

VNMGR	
Severity	Major
Log Message	Received unknown message type %d from Langley (CM socket).
Description	VN Manager status message.
Action	No action required.

VNMGR	
Severity	Major
Log Message	Heart-beat interval has expired - have missed too many heart-beats from VN Manager. VN Agent will reset all remote client information and revert to nodal operation.
Description	VN Manager status message.
Action	Indicates there is a network connectivity issue between controllers in the mobility domain. Resolve the connectivity issues for mobility to be returned to normal operation.

VNMGR	
Severity	Major
Log Message	Update interval has expired for VN Agent with IP address %s. VN Manager will remove all information for VN Agent including client session information.
Description	VN Manager status message.
Action	Indicates that there is a network connectivity issue between controllers in the mobility domain. Resolve the connectivity issues for mobility to be returned to normal operation.

H Regulatory Information

This section provides the regulatory information for the Summit WM-Series Switch and Altitude 350-2 Wireless Access Point.

Configuration of the Altitude 350-2 frequencies and power output are controlled by the regional software purchased with the Summit WM-Series controller and are downloaded from the sever upon initial set-up. A company is only allowed to download the software related it it's geographic location, thus allowing the proper set-up of Access points in accordance with local laws and regulation. The Altitude 350-2 must not be operated until proper regional software is downloaded and properly configured.

NOTE

Please refer to http://www.extremenetworks.com/go/rfcertification.htm for latest regulatory information regarding operation of the Altitude 350-2 wireless access point.

Only authorized Extreme Networks service personnel are permitted to service the system. Procedures that should be performed only by Extreme Networks personnel are clearly identified in this guide.

Changes or modifications made to the Summit WM-Series Switch or the Altitude APs which are not expressly approved by Extreme and party responsible for compliance upon installation could void the user's authority to operate the equipment.

Summit WM100 (15945), Summit WM1000 (15937)

Safety

- cULus Listed Device UL 60950-1:2001 1st Edition (North America)
- CSA C22.2 No.60950-1-03 1st Edition (Canadian Safety)
- 73/23/EEC Low Voltage Directive (LVD)
- CB Certification:
- IEC 60950-1:2001 1st Edition with applicable country deviations
- TUV-R GS Mark
- EN60950-1:2001 (European Safety)
- AS/NZS 3260 (Australia/New Zealand ACMA Safety of ITE)
- FCC 21 CFR subpart 1040.10, 1040.11 (Safety of Laser Products)
- CDRH Letter of Approval (US FDA Laser Approval)

Emissions

- FCC Part 15, Subpart B, Class A
- ICES-003, Class A
- 89/336/EEC EMC Directive
- EN 55022:1998 A2:2003 Class A (European Emissions)
- EN55024:1998 A2:2003 includes IEC/EN61000-2,3,4,5,6,11 (Europe Immunity)
- EN61000-3-2:2000 Class A (Harmonics)
- EN61000-3-3:1995 A1:2001 (Flicker)
- ETSI/EN 300 386:2001-9 (EU Telecommunication Emissions & Immunity)
- IEC/CISPR22:1997 Class A (International Emissions)
- IEC/CISPR24:1998 (International Immunity)
- IEC/EN 61000-4-2 Electrostatic Discharge
- IEC/EN 61000-4-3 Radiated Immunity
- IEC/EN 61000-4-4 Transient Bursts
- IEC/EN 61000-4-5 Surge
- IEC/EN 61000-4-6 Conducted Immunity
- IEC/EN 61000-4-11 Power Dips & Interruptions
- Australia/New Zealand AS/NZS 3548 via EU standards (ACMA)

Environmental Operating Conditions for Summit WM100/1000 and Altitude 350-2

Environmental Standards:

- EN/ETSI 300 019-2-1 v2.1.2 - Class 1.2 Storage
- EN/ETSI 300 019-2-2 v2.1.2 - Class 2.3 Transportation
- EN/ETSI 300 019-2-3 v2.1.2 - Class 3.1e Operational
- EN/ETSI 300 753 (1997-10) - Acoustic Noise
- ASTM D3580 Random Vibration Unpackaged 1.5G

Operational Environment:

- Operating Temperature Range. 0 C to +40 C (32° F to 104° F)
- Operating Relative Humidity[1] 10 - 90% RH
- Operating Altitude 0 – 3000 meters (9,850 ft)
- Operating Shock (In Rack)[1] 3G, 11ms, 60 shocks
- Operational Office Vibration (In Rack)[1] 5-100-5 Hz @ 2/10G, 0-Peak, 1 Oct./min.
- Operational Random Vibration[1] 3-500 Hz @ 1.5G rms

1. Worst-case operational condition. Not for extended use under this condition.

Storage & Transportation Environment:

- Storage & Transportation Temp.Range[1] –40° C to +70° C (-40° F to 158° F)
- Storage & Transportation Relative Humidity[1] 10 - 95% RH
- Storage & Transportation Shock[1] 18G @ 6ms, 600 shocks (package < 50kg)
- Storage & Transportation Random Vib.[1] 5-20 Hz @ 1.0 ASD w/-3dB/oct. from 20-200 Hz
- Storage & Transportation Packaging Drop[1] 14 drops min on sides & corners @ 39.4" (<15kg box)

Altitude 350-2 Integrated Antenna AP (15938), Altitude 350-2 Detachable Antenna AP (15939)

The Altitude 350-2 is Wi-Fi certified for operation in accordance with IEEE 802.11a/b/g. Certification# WFA3822.

NOTE

Operation in the European Community and rest of the world may be dependant on securing local licenses/certifications/regulatory approvals. For details and information on the most recent country-specific requirements for the Altitude 350-2, go to the following website: http://www.extremenetworks.com/go/rfcertification.htm.

United States - FCC Declaration of Conformity Statement

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

- This device may not cause harmful interference.
- This device must accept any interference received, including interference that may cause undesired operation.

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a residential and business environment. This equipment generates, uses, and radiates radio frequency energy, and if not installed and used in accordance with instructions, may cause harmful interference. However, there is no guarantee that interference will not occur. If this equipment does cause harmful interference, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the transceiver antenna.
- Increase the distance between the equipment and transceiver.

1. Worst-case Storage & Transportation condition.

- Consult the dealer or an experienced radio/TV technician for suggestion.

This equipment meets the conformance standards listed in Table 10.

Table 10: USA Conformance Standards

Safety	• UL 60950-1:2001 1st Edition, Listed Accessory	• UL 2043 Plenum Rated
EMC	• FCC CFR 47 Part 15 Class B	Tested To Comply With FCC Standards FCC ID#: RJF-A3502
Radio Transceiver	• CFR 47 Part 15.247, Class C, 2.4 GHz • CFR 47 Part 15.407, Class C, 5 GHz • CFR 47 Part 15.205, 15.207, 15.209 • CFR 47 Part 2.1091, 2.1093 • FCC OET No. 65 1997	Other: • IEEE 802.11a (5 Ghz) • IEEE 802.11b/g (2.4 GHz) • IEEE 802.3af • FCC ID: RJF-A3502
Environmental	See Environmental Conditions.	

NOTE

The Altitude 350-2 must be installed and used in strict accordance with the manufacture's instructions as described in this guide and the quick start guide for the device to which Altitude 350-2 is connected. Any other installation or use of the product violates FCC Part 15 regulations.

NOTE

The Altitude 350-2 Model 15938 with integral antenna is restricted for indoor use specifically in the UNII 5.15 - 5.25 GHz band in accordance with 47 CFR 15.407(e). The Altitude 350-2 Model 15939 with detachable antenna is disabled in the UNII 5.15 - 5.25 GHz band in accordance with 47 CFR 15.407(d).

CAUTION

This Part 15 radio device operates on a non-interference basis with other devices operating at this frequency when using integrated antennas or other Extreme Networks certified antennas. Any changes or modification to the product not expressly approved by Extreme Networks could void the user's authority to operate this device.

Conditions Under Which a Second party may replace a Part 15 Unlicensed Antenna

Second party antenna replacement (end user or second manufacturer) is permitted under the conditions listed below, with no testing or filing requirement. The general technical requirement of FCC Part 15.15 (a)(b)(c) still applies, however.

- Replacement antennas must be equal or lower then 4dBi gain within 2.4Ghz range and 5dB gain within 5GHz range. The replacement antenna must be of same type (Omnidirectional Tri band with Reverse SMA connectors) as previously authorized by the Commission/TCB.
- Replacement antennas must be the same pattern type (i.e. similar in-band and out-of-band antenna beam patterns). Special care must be taken when adhering to this condition; the antenna beam patterns of the antennas tested must be compared with the beam patterns of the replacement antennas for similarities.
- Integral and detachable antennas included with the Altitude 350-2 have been tested and included within the FCC/TCB grant. Any other antennas used with the Altitude 350-2 must follow these guidelines to be used legally with the Altitude 350-2.
- Antennas offered for sale by Extreme Networks have been tested using the highest gain of each antenna type at maximum output power.

FCC RF Radiation Exposure Statement

The Altitude 350-2 access point complies with FCC RF radiated exposure limits set forth for an uncontrolled environment. End users must follow the specific operating instructions for satisfying RF exposure compliance. This device has been tested and has demonstrated compliance when simultaneously operated in the 2.4 GHz and 5 GHz frequency ranges. This device must not be co-located or operated in conjunction with any other antenna or transmitter.

NOTE

The radiated output power of the Altitude 350-2 s far below the FCC radio frequency exposure limits as specified in "Guidelines for Human Exposure to Radio Frequency Electromagnetic Fields" (OET Bullet 65, Supplement C). This equipment should be installed and operated with a minimum distance of 20 centimeters (8 inches) between the radiator and your body or other co-located operating antennas.

Department of Communications Canada Compliance Statement

This digital apparatus does not exceed the Class B limits for radio noise emissions from digital apparatus as set out in the interference-causing equipment standard entitled "Digital Apparatus," ICES-003 of the Department of Communications.

Cet appareil numerique respecte les limites de bruits radioelectriques applicables aux appareils numeriques de Classe B prescrites dans la norme sur le materiel brouilleur: "Appareils Numeriques," NMB-003 edictee par le ministere des Communications.

This device complies with Part 15 of the FCC Rules and Canadian Standard RSS-210. Operation is subject to the following conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation. This Class B device digital apparatus complies with Canada ICES-003.

This equipment meets the following conformance standards:

Table 11: Canada Conformance Standards

Safety	• cULus Listed Accessory #60950-1-03 1st edition	• Plenum Rated Enclosure
EMC	• ICES-003 Class B	
Radio Transceiver	• RSS-210 • RSS-139-1 • RSS-102 FR Exposure • ID# 4141A-3502	Other: • IEEE 802.11a (5 GHz) • IEEE 802.11b/g (2.4 GHz) • IEEE 802.3af
Environmental	See Environmental Conditions.	

European Community

The Altitude 350-2 are wireless ports designed for use in the European Union and other countries with similar regulatory restrictions where the end user or installer is allowed to configure the wireless port for operation by entry of a country code relative to a specific country. Upon connection to the switch the software will prompt the user to enter a country code. After the country code is entered, the switch will set up the wireless port with the proper frequencies and power outputs for that country code.

Declaration of Conformity with regard to R&TTE Directive of the European Union 1999/5/EC

The symbol CE0891(!) indicates compliance with the Essential Requirements of the R&TTE Directive of the European Union (1999/5/EC). The Altitude 350-2 Integral Antenna AP (15938) and Altitude 350-2 Detachable Antenna AP (15939) models meet the following conformance standards.

Table 12: European Conformance Standards

Safety	• 73/23/EEC Low Voltage Directive (LVD) • CB Scheme, IEC 60950-1:2001 with all available country deviations	• GS Mark, EN 60950-1:2001 • Plenum Rated Enclosure
EMC	• 89/336/EEC EMC Directive	
	Emissions	
	• EN55022:1998 Class B • CISPR22:1997 Class B	• EN61000-3-2 and 3-3 • EN/ETSI 301 489-17 (9-2000)
	Immunity	
	• EN55024:1998 Class A, includes IEC 61000-4-2,3,4,5,6,11 • EN/ETSI 301 489-17 (9-2000)	
Radio Transceiver	• R&TTE Directive 1999/5/EC • ETSI/EN 300 328-2 2003-04 (2.4 GHz) • ETSI/EN 301 893-1 2002-07 (5 GHz) • ETSI/EN 301 489-1 2002-08 • ETSI/EN 301 489-17 2002-08 (RLAN)	Other: • IEEE 802.11a (5 Ghz) • IEEE 802.11b/g (2.4 GHz • IEEE 802.3af

Table 12: European Conformance Standards (Continued)

Environmental	• EN/ETSI 300 019-2-1 v2.1.2 - Class 1.2 Storage • EN/ETSI 300 019-2-2 v2.1.2 - Class 2.3 Transportation • EN/ETSI 300 019-2-3 v2.1.2 - Class 3.1e Operational • ASTM D5276 Drop Packaged • ASTM D3580 Random Vibration Unpackaged 1.5 G

NOTE

A signed copy of the Declaration of Conformity (DoC) in accordance with the preceding directives and standards has been made and is available at www.extremenetworks.com/go/rfcertification.htm.

Conditions of Use in the European Community

The Altitude 350-2 wireless access point with integrated and detachable antennas is designed and intended to be used indoors. Some EU countries allow outdoor operation with limitations and restrictions, which are described in this section. If the end user chooses to operate the Altitude 350-2 outdoors, it is their responsibility to insure operation in accordance with these rules, frequencies, and power output. The Altitude 350-2 must not be operated until proper regional software is downloaded.

WARNING!

The user or installer is responsible to ensure that he Altitude 350-2 is operated according to channel limitations, indoor / outdoor restrictions, license requirements, and within power level limits for the current country of operation. A configuration utility has been provided with the switch to allow the end user to check the configuration and make necessary configuration changes to ensure proper operation in accordance with the spectrum usage rules for compliance with the European R&TTE directive 1999/5/EC. See the switch software guide for detailed instructions on use of this utility.

The Altitude 350-2 wireless access point with integrated and detachable antennas are designed to be operated only indoors within all countries of the European Community. Some countries require limited channels of operation for indoor use. These restrictions are described in this section. For the most up to date restriction and limitations go to www.extremenetworks.com/go/rfcertification.htm.

NOTE

The Altitude 350-2 is completely configured and managed by the Summit WM-Series switch connected to the network Please follow the instructions in this software user guide to properly configure the Altitude 350-2.

- **The Altitude 350-2 wireless port requires the end user or installer to properly enter the correct country code into the switch software prior to operating the Altitude 350-2**, to allow for proper configuration in conformance with European National spectrum usage laws.
- After the first Altitude 350-2 wireless port is connected to the switch, each additional wireless port connected will inherit the operating configuration of the first Altitude 350-2 wireless port. The user or installer is responsible to ensure the first Altitude 350-2 wireless port is properly configured.
- The software within the switch will automatically limit the allowable channels and output power determined by the current country code entered. Incorrectly entering the country of operation or identifying the proper antenna used, may result in illegal operation and may cause harmful interference to other systems.
- This device employs a **radar detection feature** required for European Community operation in the 5 GHz band. This feature is automatically enabled when the country of operation is correctly configured for any European Community country. The presence of nearby radar operation may result in temporary interruption of operation of this device. The radar detection feature will automatically restart operation on a channel free of radar.
- The 5 GHz Turbo Mode feature is not enabled for use on the Altitude 350-2 Model 15938 and 15939 access point.
- The AutoChannelSelect/SmartSelect setting of the 5 GHz described in the switch software guide must always remain enabled to ensure that automatic 5 GHz channel selection complies with European requirements. The current setting for this feature is found in the 5 GHz Radio Configuration Window as described in this switch software manual.
- The Altitude 350-2 with integral or detachable antennas may be used to transmit indoors and outdoors in countries of the European Community, as indicated in Table 14.
  Go to http://www.extremenetworks.com/go/rfcertification.htm for the most up to date limitation and restrictions.
- The Altitude 350-2 must be operated indoors only when using the 5150- 5350 MHz bands, channels 36, 40, 44, 48, 52, 56, 60, or 64. See Table 13 for permitted 5 GHz channels by country.
- The Altitude 350-2 with detachable antenna must be used only with antennas certified by Extreme Networks.
- The Altitude 350-2 may be operated indoors or outdoors in all countries of the European Community using the 2.4 GHz band: Channels 1 – 13, except where noted in Table 14.
- In Italy, the end user must apply for a license from the national spectrum authority to operate this device outdoors.
- In Belgium, outdoor operation is only permitted using the 2.46 - 2.4835 GHz band: Channel 13.
- In France, outdoor operation is only permitted using the 2.4 - 2.454 GHz band: Channels 1 - 7.

Permitted 5 GHz Channels for the European Community

Table 13 lists the 5 GHz channels approved for operation in the European Community.

Table 13: Permitted 5 GHz Channels in European Community Countries

Permitted Frequency Bands	Permitted Channel Numbers	Countries
5.15-5.25GHz	36, 40, 44, 48	Austria, Belgium
5.15-5.35GHz	36, 40, 44, 48, 52, 56, 60, 64	France, Switzerland, Liechtenstein
5.15-5.35* & 5.470-5.725GHz	36, 40, 44, 48, 52, 56, 60, 64, 100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140	Denmark, Finland, Germany, Iceland, Ireland, Italy, Luxembourg, Netherlands, Norway, Portugal, Spain, Sweden, U.K.
5GHz Operation Not Allowed	None	Greece

European Spectrum Usage Rules

Table 14 lists the rules and restrictions for operating a 2.4 GHz or 5 GHz device in the European Community. Always use the latest software version for the most up-to-date channel list; some earlier software versions supply only a limited number of channels.

The Altitude 350-2 must be installed in the proper indoor or outdoor location. Use the installation utility provided with the switch software to insure proper set-up in accordance with all European spectrum usage rules.

Table 14: European Spectrum Usage Rules - Effective as of July 2005

Country	5.15-5.25 (GHz) Channels: 36,40,44,48	5.25-5.35 (GHz) Channels: 52,56,60,64	5.47-5.725 (GHz) Channels: 100,104,108,112,116,120,124,128,132,136,140	2.4-2.4835 (GHz) Channels: 1 to 13 (Except Where Noted)
Austria	Indoor Only	Indoor Only	Indoor or Outdoor	Indoor or Outdoor
Belgium[a]	Indoor Only	Indoor Only	Indoor or Outdoor	Indoor or Outdoor[a]
Bulgaria	Indoor Only	Indoor Only	Indoor or Outdoor	Indoor or Outdoor
Denmark	Indoor Only	Indoor Only	Indoor or Outdoor	Indoor or Outdoor
Cyprus	Indoor Only	Indoor Only	Indoor or Outdoor	Indoor or Outdoor
Czech Rep.	Indoor Only	Indoor Only	Expect to Open Fall 2006	Indoor or Outdoor
Estonia	Indoor Only	Indoor Only	Indoor or Outdoor	Indoor or Outdoor
Finland	Indoor Only	Indoor Only	Indoor or Outdoor	Indoor or Outdoor
France	Indoor Only	Indoor Only	Expect to Open Fall 2006	Indoor channels 1-13 **Outdoor channels 1-7 only**
Germany	Indoor Only	Indoor Only	Indoor or Outdoor	Indoor or Outdoor
Greece	Indoor Only	Indoor Only	Indoor Only	Indoor Only
Hungary	Indoor Only	Indoor Only	Indoor or Outdoor	Indoor or Outdoor
Iceland	Indoor Only	Indoor Only	Indoor or Outdoor	Indoor or Outdoor
Ireland	Indoor Only	Indoor Only	Indoor or Outdoor	Indoor or Outdoor
Italy	Indoor Only	Indoor Only	Indoor (Outdoor w/License)	Indoor (Outdoor w/License)
Latvia	Indoor Only	Indoor Only	Indoor or Outdoor	Indoor or Outdoor

Table 14: European Spectrum Usage Rules - Effective as of July 2005 (Continued)

Country	5.15-5.25 (GHz) Channels: 36,40,44,48	5.25-5.35 (GHz) Channels: 52,56,60,64	5.47-5.725 (GHz) Channels: 100,104,108,112,116,120,124,128,132,136,140	2.4-2.4835 (GHz) Channels: 1 to 13 (Except Where Noted)
Liechtenstein	Indoor Only	Indoor Only	Indoor or Outdoor	Indoor or Outdoor
Lithuania	Indoor Only	Indoor Only	Indoor or Outdoor	Indoor or Outdoor
Luxembourg	Indoor Only	Indoor Only	Indoor or Outdoor	Indoor or Outdoor
Netherlands	Indoor Only	Indoor Only	Indoor or Outdoor	Indoor or Outdoor
Malta	Indoor Only	Indoor Only	Indoor or Outdoor	Indoor or Outdoor
Norway	Indoor Only	Indoor Only	Indoor or Outdoor	Indoor or Outdoor
Poland	Indoor Only	Indoor Only	Indoor or Outdoor	Indoor or Outdoor
Portugal	Indoor Only	Indoor Only	Indoor or Outdoor	Indoor or Outdoor
Slovak Rep.	Indoor Only	Indoor Only	Indoor or Outdoor	Indoor or Outdoor
Slovenia	Indoor Only	Indoor Only	Indoor or Outdoor	Indoor or Outdoor
Spain	Indoor Only	Indoor Only	Indoor or Outdoor	Indoor or Outdoor
Sweden	Indoor Only	Indoor Only	Indoor or Outdoor	Indoor or Outdoor
Switzerland	Indoor Only	Indoor Only	Indoor or Outdoor	Indoor or Outdoor
U. K.	Indoor Only	Indoor Only	Indoor or Outdoor	Indoor or Outdoor
Turbo Mode	Not Allowed in 5GHz	Not Allowed in 5GHz	Not Allowed in 5GHz	Same 2.4 GHz rules as above
AdHoc Mode	Not Allowed	Not Allowed	Not Allowed	Same 2.4 GHz rules as above

a. Belgium requires that the spectrum agency be notified if you deploy wireless links greater than 300 meters in outdoor public areas using 2.4 GHz band.

Declarations of Conformity

Table 15 presents the Extreme Networks declarations of conformity for the languages used in the European Community.

Table 15: Declaration of Conformity in Languages of the European Community

English	Hereby, Extreme Networks, declares that this Radio LAN device is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.
Finnish	Valmistaja Extreme Networks vakuuttaa taten etta Radio LAN device tyyppinen laite on direktiivin 1999/5/EY oleellisten vaatimusten ja sita koskevien direktiivin muiden ehtojen mukainen.
Dutch	Hierbij verklaart Extreme Networks dat het toestel Radio LAN device in overeenstemming is met de essentiele eisen en de andere relevante bepalingen van richtlijn 1999/5/EG Bij deze verklaart Extreme Networks dat deze Radio LAN device voldoet aan de essentiele eisen en aan de overige relevante bepalingen van Richtlijn 1999/5/EC.
French	Par la presente Extreme Networks declare que l'appareil Radio LAN device est conforme aux exigences essentielles et aux autres dispositions pertinentes de la directive 1999/5/CE Par la presente, Extreme Networks declare que ce Radio LAN device est conforme aux exigences essentielles et aux autres dispositions de la directive 1999/5/CE qui lui sont applicables
Swedish	Harmed intygar Extreme Networks att denna Radio LAN device star I overensstammelse med de vasentliga egenskapskrav och ovriga relevanta bestammelser som framgar av direktiv 1999/5/EG.
Danish	Undertegnede Extreme Networks erklarer herved, at folgende udstyr Radio LAN device overholder de vasentlige krav og ovrige relevante krav i direktiv 1999/5/EF
German	Hiermit erklart Extreme Networks, dass sich diese Radio LAN device in Ubereinstimmung mit den grundlegenden Anforderungen und den anderen relevanten Vorschriften der Richtlinie 1999/5/EG befindet". (BMWi) Hiermit erklart Extreme Networks die Ubereinstimmung des Gerates Radio LAN device mit den grundlegenden Anforderungen und den anderen relevanten Festlegungen der Richtlinie 1999/5/EG. (Wien)
Greek	*ΜΕ ΤΗΝ ΠΑΡΟΥΣΑ Extreme Networks ΔΗΛΩΝΕΙ ΟΤΙ* Radio LAN device *ΣΥΜΜΟΡΦΩΝΕΤΑΙ ΠΡΟΣ ΤΙΣ ΟΥΣΙΩΔΕΙΣ ΑΠΑΙΤΗΣΕΙΣ ΚΑΙ ΤΙΣ ΛΟΙΠΕΣ ΣΧΕΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ ΤΗΣ ΟΔΗΓΙΑΣ 1999/5/ΕΚ*
Italian	Con la presente Extreme Networks dichiara che questo Radio LAN device e conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttiva 1999/5/CE.
Spanish	Por medio de la presente Extreme Networks declara que el Radio LAN device cumple con los requisitos esenciales y cualesquiera otras disposiciones aplicables o exigibles de la Directiva 1999/5/CE
Portuguese	Extreme Networks declara que este Radio LAN device esta conforme com os requisitos essenciais e outras disposicoes da Directiva 1999/5/CE.

Certifications of Other Countries

The Altitude 350-2 Model 15938 and 15939 wireless port has been certified for use in the countries listed in Table 16. When the Altitude 350-2 is connected to the Extreme Networks switch, the user is prompted to enter a country code. Once the correct country code is entered, the switch automatically sets up the Altitude 350-2 with the proper frequencies and power outputs for that country code.

Go to http://www.extremenetworks.com/go/rfcertification.htm for the most up to date list of certified countries.

NOTE

It is the responsibility of the end user to enter the proper country code for the country the device will be operated within.

Table 16: Other Country Specific Compliance Standards, Approvals and Declarations

Country	Standards, Approvals, Declarations	
Australia and New Zealand	• Altitude 350-2 (with Integrated or Detachable Antenna) • AS/NZS 4288 (Radio) • AS/NZX 3260 (Safety) • AS/NZS 3548 (Emissions) • EEE 802.11a/b/g • IEEE 802.3af (PoE)	ACN 090 029 066 • EN 300 328-2:2003-4 (2.4 GHz) • EN 301 893-1:2003-08 (5 GHz) • EN 301 489-17:2002-08 (RLAN) • EN 60950-1:2001 with Australia Deviation

Index

A

access approval
  Altitude AP, in discovery, 49
accounting
  setup on a WM-AD, 84
adding
  a new WM-AD subnet name, 66
  Altitude AP manually, 56
  RADIUS server definitions, 69
alarms
  overview of log types and levels, 140
allow all or approved APs
  for availability setup, 104
  for discovery and registration, 44
allow or deny in a filtering rule, 65
Altitude AP
  access approval, 49
  adding for availability setup, 104
  adding manually, 56
  assigning to a WM-AD, 72
  client blacklist, 135
  client disassociate, 133
  configure for a WM-AD for voice traffic, 102
  connecting and powering, 44
  enabling Telnet for debugging, 181
  LED sequence in discovery, 48
  maintenance and reboot, 131
  radios, 42, 52
  static configuration, 57
  view statistics, 145
Analysis engine
  functions, 126
  overview of Summit Spy feature, 123
antennae on the Altitude AP, 42
audits
  view GUI audits, 143
authentication
  MAC-based, 82
  no RADIUS server, 61
  none on a WM-AD, 100
  on a WM-AD for AAA, 82
  on a WM-AD for Captive Portal, 77
  overview of types, 76
  protocols supported, 63, 79
Authentication, Authorization, Accounting (AAA)
  filter ID values (RADIUS policy), groups, 85
  set up 802.1x authentication, 82
  set up a WM-AD topology, 75
  set up privacy on a WM-AD, 97
Auto Cell, 58

B

blacklist a wireless client, 135
branch office, static configuration of Altitude AP, 57
bridge traffic locally, branch office, 58

C

call data records (CDRs), 84
Captive Portal
  authentication on a WM-AD, 77
  configuring internal, 80
  defined, 63
  filter ID values (RADIUS policy), 85
  non-authenticated filtering rules, 87
  privacy mechanisms, 96
  set up a WM-AD topology, 71
  view sample page, 81
Check Point event logging, 113
configuring
  a new WM-AD, 66
  Captive Portal, internal, 80
  data ports, 32
  software - overview steps, 31
  static routes, 35

D

data port interfaces
  configuring, 32
default filter, 92
default gateway on a WM-AD, 73
disassociate a wireless client, 133
discovery
  Altitude AP LED sequence, 48
  registration settings, 44
  steps, 46
displays
  Altitude AP availability, 105
  Altitude AP wired and wireless statistics, 145
  client location by foreign SWM, 109
  client location by home, 109
  list of displays, 144

SWM tunnel traffic, 109
documentation feedback, 10
Domain Name Server (DNS)
in discovery, 46
Dynamic Host Configuration Protocol (DHCP)
for availability, 103
for mobility (WM-AD Manager), 107
Option 78 in discovery, 46
relay on a WM-AD, 74
required as part of solution, 15

E

event logging
in Check Point, 113
in SWM software, 140
exception filters
on a WM-AD, 87
port-based, 39
exclusions, IP address range on a WM-AD, 73

F

failover of a RADIUS server, 79
failover of a Summit WM-Series Switch
availability overview, 22
events and recovery, 106
ferrite beads, installing on Controller cables, 24
filtering
default filter, 92
exception filter on a WM-AD, 87
filtering rules, overview of set up, 86
for an AAA group, 94
for Captive Portal authentication, 81
non-authenticated filter for Captive Portal, 87
non-authenticated filtering rules, examples, 89
on a WM-AD for third-party APs, 120
overview of packet filtering, 21
overview, four types, 64
port-based, 39
rules forFilter ID values, 90
set Filter ID values (RADIUS policy), 84
foreign Altitude APs, for availability, 49, 72
formatting conventions, 10
forwarding table report, 36
friendly APs, Summit Spy feature, 128

G

gateway, default, on a WM-AD, 73
global settings
for a WM-AD, 68
priority traffic handling on a WM-AD, 102
RADIUS servers for authentication, 78
graphical user interface (GUI)
main menu, 26
overview, 28
view audit log, 143
groups for Authentication, Authorization, Accounting (AAA), 85

H

health checking status of Altitude APs, 135
heartbeat messages, in WM-AD Manager feature, 107

I

installing
Altitude AP, 43
Summit WM-Series Switch, 24
IP address range on a WM-AD, 73

L

LED sequence
in discovery, 48
local Altitude APs, for availability, 49
login user name and password, 26
Login-LAT-Group, 90
for WM-AD AAA authentication, 85
logs
changing log level, 135
event logging in Check Point, 113
overview of types and levels, 140

M

MAC-based authentication, 82
main menu, 26
Management Information Bases (MIBs) supported, 115
management port
first-time setup, 24
management traffic on data port, 33
modify management port settings, 27
port-based filtering, 39
management traffic
enabling on a WM-AD, 73
mobility
overview, 21
WM-AD Manager and WM-AD Agent, 107
MTU (Maximum Transmission Unit)
in data port setup, 32
multicast
for a WM-AD, 95
set up a WM-AD for VoIP, 102

N

network assignment
by AAA, 75, 97
by SSID for Captive Portal, 71
options for a WM-AD, 63
network time synchronization, 112
next hop route for a WM-AD, 73
non-authenticated filter for Captive Portal, 81, 87

O

operating system software upgrade, 137
OSPF
configuring, 36
linkstate report, 38
neighbor report, 38
on a WM-AD, 73

P

paired Summit WM-Series Switch for availability, 104
port
configuring data ports, 32
management, first-time setup, 24
port exception filters, 39
power supply, Summit WM-Series Switch, 24
powering
Altitude AP, 44
priority traffic handling
enable for a WM-AD, 102
privacy
dynamic WEP on a WM-AD for AAA, 98
encryption methods supported, 19
on a WM-AD for AAA
AAA, 97
overview on a WM-AD, 66
setup on a WM-AD for Captive Portal, 96
static WEP for an AAA WM-AD, 98
WPA v1 and WPA v2 on a WM-AD for AAA, 98
product key
enabling, 31
part of maintenance screen, 137
protocols
for authentication by Captive Portal, 79
supported, overview, 11

R

radio
5 GHz (a) and 2.4 GHz (b/g), 42
Auto Cell, 58
channels, 55
RF scanner, 123
radio settings
view and modify, 52
RADIUS server
defining servers in global settings screen, 69
deployment with no server, 61
Filter ID values, 90
for authentication, 78
for MAC-based authentication, 82
priority for redundancy, 79
RADIUS accounting, 84
RADIUS policy for a WM-AD, 84
required as part of solution, 15
VSAs in RADIUS message, 77
read/write privileges, 111
reboot Altitude AP, 131
registration
settings for availability setup, 104
settings for discovery process, 44
regulatory information, 11
reports
AP inventory, 146
forwarding table, 36, 146
list of displays, 144
OSPF linkstate, 38, 146
OSPF neighbor, 38, 146
restore Summit WM-Series Switch software configuration, 140
RF Data Collector (RFDC), 123
RF scans, Summit Spy feature, 125
rogue detection, Summit Spy feature, 127
routing
configuring OSPF on data port, 36
configuring static routes, 35
next hop route on a WM-AD, 73
overview, 20
routing table
viewing, 36

S

safety compliances, 11
scan results, Summit Spy feature, 127
scanning RF via the Summit Spy feature, 125
security clip and rivet on the Altitude AP bracket, 43
security of network, overview of methods, 19
Service Location Protocol (SLP)
for availability, 103
for mobility (WM-AD Manager), 107
in discovery, 46
required as part of solution, 15
traffic allowed on data port, 33
view slpdump tool report, 106
set up for a WM-AD, 119

shut down system, 135
Simple Network Management Protocol (SNMP)
  enabling, 116
  MIBs supported, 115
software
  maintenance of Altitude AP software, 131
  maintenance of Summit WM-Series Switch software, 137
SSID network assignment for Captive Portal, 71
standards supported, 11
static configuration of Altitude AP, 57
static routes
  configuring, 35
  viewing forwarding table report, 36
status of Altitude APs in Access Approval screen, 49
Summit WM-Series Switch
  availability overview, 22
  define management user names, passwords, 111
  define network time synchronization, 112
  defined as WM-AD Manager for mobility, 107
  enable ELA event logging (Check Point), 113
  enabling SNMP, 116
  events during a failover, 106
  installing, 24
  paired for availability, 103
  restore software configuration, 140
  set up third-party APs, 119
  software maintenance, product key, 31
  system maintenance, 135
  system shutdown, 135
Summit WM-Series Switch software configuration, 139
syslog event reporting
  define parameters, 135

T

Telnet, configuring and enabling for the AP, 181
third-party APs, 119
  defining a WM-AD for, 73
  in Summit Spy feature, 129
topology of a WM-AD
  AAA, 75
  Captive Portal, 71
traces
  overview of log types and levels, 140
Type of Service (ToS/DSCP)
  part of Quality of Service, 22

U

user name and password for login, 26

V

vendor specific attributes (VSA)
  in RADIUS message, 77
  RADIUS server
    vendor specific attributes, 79
Voice-over-IP (VoIP)
  define multicast groups on a WM-AD, 95
  set up a WM-AD for, 101

W

Wi-Fi Multimedia (WMM)
  part of Quality of Service, 22
Wi-Fi Protected Access (WPA)
  overview on a WM-AD, 66
  PSK mode for Captive Portal, 97
  WPA v1 and v2 on a WM-AD for AAA, 98
Wired Equivalent Privacy (WEP)
  on a WM-AD for AAA, 98
  overview on a WM-AD, 66
  static for Captive Portal, 96
WM Access Domain Services (WM-AD)
  authentication by AAA (802.1x), 82
  authentication by Captive Portal, 77
  creating a new WM-AD, 66
  define filtering rules, 86
  defined, 62
  for third-party APs, 120
  global settings, 68
  multicast, 95
  network assignment overview, 63
  overview, 20
  privacy for AAA, 97
  privacy overview, 96
  set up for VoIP, 101
  topology for AAA, 75
  topology for Captive Portal, 71
WM-AD Manager
  defining a Summit WM-Series Switch for mobility, 107